Proyecto Fin de Grado
Grado en Ingeniería de las Tecnologías de la Telecomunicación

Despliegue de una red inalámbrica, mejora de la red de área local e integración con la Red Corporativa

Autor: Valle Naranjo Cano

Tutor: Juan Manuel Vozmediano Torres

Departamento de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2018

Proyecto Fin de Grado

Grado en Ingeniería de las Tecnologías de la Telecomunicación

Despliegue de una red inalámbrica, mejora de la red de área local e integración con la Red Corporativa

Autor:

Valle Naranjo Cano

Tutor:

Juan Manuel Vozmediano Torres

Profesor Titular de Universidad

Departamento de Ingeniería Telemática

Escuela Técnica Superior de Ingeniería

Universidad de Sevilla

Sevilla, 2018

Proyecto Fin de Grado: Despliegue de una red inalámbrica, mejora de la red de área local e integración con la Red Corporativa

Autor: Valle Naranjo Cano
Tutor: Juan Manuel Vozmediano Torres

El tribunal nombrado para juzgar el trabajo arriba indicado, compuesto por los siguientes profesores:

Presidente:

Vocal/es:

Secretario:

acuerdan otorgarle la calificación de:

El Secretario del Tribunal

Fecha:

A esa niña pequeña que un día soñó con esto ...

Agradecimientos

"Cuando eres pequeño te preguntan muy a menudo, ¿y tú? ¿Qué quieres ser de mayor?" eso es lo que me cuestionaba un par de meses después de comenzar la carrera. Y ahora estoy a punto de dar respuesta a esa pregunta, eso sí, esta respuesta es simplemente una primera aproximación, aún me queda mucho a lo que responder. Para resolver cualquier pregunta de un problema se cuenta con determinadas ecuaciones y teoremas que ayudan a dar con la solución. Estas han sido las mías a lo largo de estos años.

- "Teorema de Pitágoras"

  Todos aquellos docentes que más que profesores con el tiempo se convirtieron en familia. Gracias por crear en mí la base inicial en la que se fundamenta todo, por poner el primer granito de arena. Isaac Naz, por todos los consejos, Raquel Hernández, por aquel café en la estación lleno de consejos y energía, Javier Blasco, por abrirme el camino.

- "Los logaritmos"

  Papá, gracias por hacerme creer en los sueños y por apoyarme e insistir tanto en que cumpla los míos. Gracias por inculcar en mí la magia de la vida, por estar siempre al otro lado del teléfono con un "¿Dónde está lo más bonito del mundo mundial?". Gracias por enseñarme tu fortaleza, pero sobre todo por confiar en mí cada minuto incluso en los momentos en los que yo no lo hacía. Siempre serás mi ejemplo a seguir.

- "Raíz cuadrada de -1"

  Mamá, pilar fundamental de mi mundo, es tu fuerza y valentía ante la vida la que hoy me hace estar aquí. Tú mamá, eres la voz capaz de tranquilizarme en todos los momentos de mi vida. Gracias por entenderme y respetarme tal y como soy, en cualquier momento y en cualquier lugar, por todas y cada una de las llamadas de auxilio, las charlas, los consejos y los llantos, pero sobre todo por las respuestas de calma, de energía, de besos y de animo. Gracias por levantarme todas las veces que he caído y que no encontraba el camino a seguir. Siempre serás mi ejemplo a seguir.

- "Transformada de Fourier"

  AA, no te llegas a imaginar lo feliz que me hace que quieras seguir mis pasos, solo espero no decepcionarte nunca. Gracias por todos esos consejos durante los viajes en coche, cuando las conversaciones son solo nuestras.

- "Teorema de Shannon"

  Mi familia, mi hogar. Gracias tito grande, tito chico y tita Vanesa, gracias por creer en mí y por escucharme con cada problema que os contaba en las sobremesas de los sábados. Gracias abuela y tres estrellas del cielo porque, aunque nunca he conseguido poder explicaros que es lo que estaba

estudiando vuestra nieta, siempre me habéis hecho más fuerte.

- “Fórmula de Euler”

  Carlos y Armando, gracias por esos ratitos que nos alegran la vida, por hacerme parte de vosotros aunque pase el tiempo, por soñar conmigo desde que compartíamos caramelos en preescolar, pero sobretodo por entender cada uno de mis "Lo siento chicos, pero hoy no puedo, estoy estudiando".

- “Teorema de muestreo de Nyquist”

  Cuarteto Chicas Teleco, gracias por entrar en mi vida y por regalarme momentos tan perfectos, tan nuestros, tan para nosotras, aquí, allí, en el Coliseo Romano cantando "Adelante por los sueños que aún nos quedan. . . ", en la biblioteca rodeadas de nervios y estrés, en mitad del mediterráneo bailando como si no hubiera un mañana, o en un "baño" repleto de confesiones y secretos. Un día decidimos olvidarnos de todos esos "puff" que venían justamente después de decir que estudiábamos teleco, y nos lanzamos a la aventura juntas, gracias por ser la excepción que confirma la regla. Porque sois otra parte más de mi familia.

- "Funciones trigonométricas"

  Hombres de mi vida, gracias por tener un hueco en vuestras vidas para mí. Kikiño gracias por cada risa, por recogerme el primer día de Universidad sin conocernos, por cada proyecto, práctica o trabajo, por cada regañá que cogía a hurtadillas, por cada boli que te he robado, pero sobretodo por ayudarme con cada piedra con la que tropezaba porque tú siempre ves el lado bueno de las cosas. Chu, gracias por tener siempre un consejo para mí y en cualquier circunstancia, por haberme entendido desde el minuto uno, por todos los abrazos que sin decir que los necesitaba me has regalado, por estar siempre y por todos los momentos. Danichurri, gracias por seguir a mi lado durante la carrera a pesar de tener que leer mis apuntes en espiral, por alegrarme las mañanas, por tener siempre una palabra bonita para mí.

- "¿Qué es Internet?"

  Teleñecos, gracias por todos y cada uno de los proyectos, horas de agobios y exámenes que hemos compartido, sobre todo por aguantar hasta mis "Levantaaaaaaarse" y ponerlos de politono.

- “Relación señal/ruido”

  Sandetel, gracias a cada una de las personas que me han permitido absorber un poquito de su sabiduría, gracias por creer y confiar en mí, porque poner un pie en el Cubo fue un bonito y gran cambio de chip. Gracias Carlos y Pedro por darme la oportunidad de formar parte de todo, gracias Mome por considerarme siempre "uno" más, gracias Soltelianos por acogerme en el equipo, gracias Javi, por hacerme sentir como en casa y hacer el "cuadradito" mucho más acogedor, nunca olvidaré como crimpar un cable.

- "Protocolos de Señalización"

  Gracias a mi tutor y profesor, Juan Manuel Vozmediano por la paciencia y los consejos tras cada visita, por hacerme cambiar de idea en algunos aspectos, con lo difícil que resulta eso, por llamarme cabezota y hacerme pensar. Gracias por aquel "Valle, ¿no estarás con el móvil verdad?", en la primera clase de "Protocolos" de segundo.

Valle Naranjo Cano

Sevilla, 2018

Resumen

El presente documento tiene por objeto la integración de una nueva sede a la Red Corporativa que interconecta todas las sedes de la empresa con la que se trabaja en este proyecto, lo que desemboca en la mejora del cableado e infraestructura existente, de la electrónica de red (LAN) y la creación de un sistema de acceso inalámbrico (WLAN) en ella.

Durante el desarrollo del proyecto se intenta llegar a la mejor solución para la implementación de la red, por lo que se presentan y definen cada una de las etapas en las que se divide el proyecto; toma de requisitos, análisis, diseño, configuración, suministro e instalación.

Cada uno de estos procesos ha sido dividido en tres bloques; cableado estructurado, LAN y WLAN, con la finalidad de poder hacer frente a las necesidades planteadas de la forma más detallada posible y buscando la mejor solución para cada uno de los problemas y requisitos.

Tras la conclusión e instalación del proyecto se consigue unificar y centralizar todos los servicios que se ofrecen a las sedes de la empresa así como la autenticación de usuarios, asignación y gestión del direccionamiento IP y monitorización. Además con los cambios que se llevan a cabo en la red inicial, se mejoran las prestaciones de seguridad, disponibilidad y rendimiento de los usuarios, cumpliendo con todas las necesidades del cliente.

Abstract

The purpose of this document is to integrate a new headquarters into the Corporate Network that interconnects all the headquarters of the company with which this project is being worked on, which leads to the improvement of the existing cabling and infrastructure of the network electronics (LAN) and the creation of a wireless access system (WLAN) in it.

During the development of the project, we try to arrive at the best solution for the implementation of the network, which is why we present and define each of the stages in which the project is divided; taking of requirements, analysis, design, configuration, supply and installation.

Each of these processes have been divided into three blocks; structured wiring, LAN and WLAN, in order to meet the needs outlined in the most detailed way possible and seeking the best solution for each of the problems and requirements.

After the conclusion and installation of the project it is possible to unify and centralize all the services offered to the company's headquarters, as well as user authentication, assignment and management of IP addressing and monitoring. In addition to the changes that are carried out in the initial network, the security, availability and performance of the users are improved, fulfilling all the needs of the client.

Índice

Índice de Figuras

Índice de Tablas

1 Introducción

"¿Y por qué no?"

ANTONIO ÁNGEL NARANJO CANO

1.1 Introducción

Actualmente las empresas tienden al desarrollo de una Red Corporativa que les permite desplegar un conjunto unificado de servicios avanzados, obteniendo soluciones más potentes e innovadoras y reduciendo los costes globales en telecomunicaciones. Así nace la Red Corporativa de Telecomunicaciones de la empresa con la que se trabaja en este proyecto.

Esta se dedica a la prestación de servicios vinculados al espacio público de parques y jardines, así como, la coordinación y gestión de las actividades urbanas que se realizan en ellos. La empresa está constituida por las sedes de cada uno de estos parques y jardines distribuidos por todo el territorio de la comunidad autónoma.

La gestión de las telecomunicaciones de esta empresa antes de la creación de la Red Corporativa estaba basada en múltiples contratos, ya que los servicios se gestionaban a nivel de sede, lo que desembocaba en un elevado gasto.

Al unificar todas las redes de telecomunicaciones existentes se consigue:

- Puesta en marcha de nuevos servicios.

  Muchas de las sedes, las de reducido número de trabajadores, podrían acceder a servicios y prestaciones que no tenían accesible con anterioridad puesto que con la nueva red los servicios ofrecidos son homogéneos.

- Centralización de la gestión de la red.

  El control de la Red Corporativa y de todas las sedes que se integran en ella, tienen una gestión centralizada desde un único servidor.

- Mayor capacidad de análisis.

  Al proyectar todos los equipos de las sedes contra un mismo punto, es posible realizar un análisis del estado de la seguridad en la totalidad de la red.

- Comunicación privada.

  Esta red permite la comunicación entre todas las sedes sin la necesidad de salir a Internet.

1.2 Motivación y Objetivos

Tras la incorporación de un nuevo parque a la empresa, se cuenta con una nueva sede que debe vincularse a la Red Corporativa.

El presente proyecto tiene como objetivo la mejora de la red existente en la sede, así como, el estudio, configuración e implantación de una red de área local inalámbrica (WLAN). Además el propósito más relevante reside en la integración con la Red Corporativa anteriormente mencionada.

Los objetivos del proyecto serán:

- Interconectar la nueva sede a la Red Corporativa de la empresa.
- Actualizar la arquitectura LAN existente además del cableado estructurado que sea necesario.
- Dotar de cobertura inalámbrica a todas las instalaciones del edificio, así como a la explanada que se encuentra frente a su fachada exterior.
- Interconectar la red LAN existente con la nueva WLAN, permitiendo la conexión lógica de las mismas.
- Aportar tres tipos de servicio:
  - Acceso a los recursos compartidos, servicios horizontales e Internet para los empleados del parque (a partir de ahora se denominan EMPLEADOS).
  - Acceso a los recursos compartidos e Internet para los empleados de otras sedes de la empresa (a partir de ahora se denominan ITINERANTES).
  - Acceso a Internet para los visitantes del parque (a partir de ahora se denominan INVITADOS).
- Proporcionar altas capacidades en cuanto a seguridad, control del tráfico, control del direccionamiento y redundancia.
- Suministrar una gestión y autenticación centralizada que nos garantiza un alto nivel de rendimiento.

1.3 Metodología y plan de trabajo

El método de trabajo ha sido analizar las necesidades de la sede, estudiar la situación en la que se encuentra y definir la solución más acertada detallando los servicios ofrecidos y configurados, así como, la arquitectura elegida para su desarrollo. Los pasos que se siguen para cumplir los objetivos propuestos se detallan a continuación.

1.3.1 Toma de requisitos

- Primeras reuniones, entrevistas y correos

  El primer paso reside en planificar las entrevistas con el personal responsable de la sede e intercambiar numerosos correos con toda la información necesaria. El resultado se traduce en conocer la situación en la que se encuentra y las necesidades que se deben suplir.

  Estas reuniones permiten tener una primera toma de contacto y conocer datos relevantes sobre el lugar, como son el material de las paredes del edificio o la existencia de falso techo.

- Documentación

  La documentación es necesaria para conocer las características y peculiaridades que tiene la sede, destacando los planos de las zonas donde se quiere integrar la red WiFi. La recopilación de informes y auditorías ayudan a conocer la arquitectura inicial con la que cuenta, contextualizar y poder diseñar en fases posteriores una primera versión de la red.

- Toma de requisitos

  Las necesidades y exigencias de la sede son recapituladas para poder delimitar todas las peticiones.

- Estudio de la normativa vigente

  El estudio de las recomendaciones, reglas y leyes en vigor sobre las políticas de seguridad para redes Wi-Fi es un punto muy relevante en el proyecto ya que determina limitaciones en la red.

1.3.2 Fase de análisis

- Análisis de la situación inicial

  El análisis inicial se realiza dividiendo el proyecto en tres bloques: cableado estructurado, LAN y WLAN.

  Los dos primeros son objeto de un estudio a fondo de los elementos que la forman, analizando cuáles pueden reutilizarse y cuáles sustituirse.

  El tercer bloque supone un desarrollo desde el inicio de una red inalámbrica, por lo que a partir de la información recogida sobre el terreno se ejecutan los primeros estudios de cobertura, se estudia la arquitectura actual y los requisitos de la sede.

- Estimación técnica inicial

  Esta primera aproximación recoge todas las conclusiones a las que se llega tras el estudio previo, con lo que se elabora un diseño inicial con las primeras versiones de cada uno de los tres bloques.

- Aprobación inicial por parte del cliente

  El diseño inicial debe ser aprobado por los responsables de la sede ya que no se puede pasar a etapas sucesivas si no se aceptan las condiciones que se plantean en esta primera versión. Una vez se tenga su consentimiento se continúa trabajando para crear el diseño final.

1.3.3 Fase de Diseño

- Replanteo final y segundo estudio de cobertura

  Realizar un replanteo final de los puntos de acceso y de los equipos centrales de la red es lo que permite corroborar o mejorar la viabilidad de la primera aproximación. Este replanteo se lleva a cabo in situ, lo que hace mucho más veraz los resultados y permite ejecutar un nuevo estudio de cobertura.

- Elección y compra del equipamiento

  El análisis y estudio de todo el equipamiento Wi-Fi existente en el mercado lleva a la selección de aquel que cumple con las necesidades planteadas y ofrece las mejores prestaciones. Este mismo proceso de análisis, estudio y selección también se sigue para el cableado estructurado.

- Diseño final

  El último paso es la realización de un planteamiento final de la arquitectura de red, donde se detallan los servicios con los que contará este diseño y describe las soluciones a nivel 2 y nivel 3.

1.3.4 Fase de despliegue

- Configuración

  Este punto recoge toda la configuración de los puntos de acceso, las controladoras, el direccionamiento y cada uno de los servicios existentes en la red Wi-Fi.

  El sistema de monitorización también es configurado, es un sistema centralizado y común para todas las sedes que forman parte de la Red Corporativa de la empresa.

- Instalación

  Una vez que la configuración ha sido realizada el paso posterior es la instalación de los equipos, cableado e infraestructuras auxiliar.

1.3.5 Fase de pruebas y monitorización

- Pruebas de verificación

  Las pruebas son utilizadas para verificar y comprobar que las configuraciones realizadas son las correctas, y que los servicios funcionan con normalidad. Este estudio se lleva a cabo in situ, además se cuenta con la ayuda del sistema centralizado de monitorización con el que se controla tanto los puntos de acceso como las controladoras, observando su rendimiento y estado.

- Documentación

  Para finalizar, toda la información necesaria del nuevo despliegue es documentada.

  Durante la vida del proyecto se realiza una labor de seguimiento, en la que es posible la solución a diferentes problemas y consultas que puedan surgir.

1.4 Equipo de trabajo

El grupo de personas que realizan el trabajo se describe en este apartado, explicando cada uno de los perfiles que lo integran y detallando las responsabilidades de cada miembro que participa en el proyecto.

El equipo de trabajo que se dedica a desarrollar la solución más efectiva para este desarrollo WiFi y los servicios Corporativo e Invitado está compuesto por:

- Jefe de Proyecto, cuyas funciones son:
  - Velar por el cumplimiento de los objetivos y requisitos del proyecto.
  - Organizar los recursos de manera que la prestación de los servicios sea óptima.
  - Realizar informes de actividades o seguimientos.
  - Preparar y dirigir todas las reuniones con el cliente.
  - Gestionar las actividades para el desarrollo del proyecto.
  - Determinar y responsabilizarse los costes, plazos, desarrollo, resultados y cualquier desviación que pueda surgir.

- Ingeniero de Red Experto en WLAN y LAN, cuyas funciones son:
  - Revisar que la infraestructura asignada está configurada y tiene un correcto funcionamiento.
  - Analizar la red desde el punto inicial hasta llegar a la solución más óptima.
  - Diseñar la solución de la red.
  - Elegir el equipamiento más apropiado que cumple con las necesidades del cliente y las especificaciones técnicas que requiere.
  - Realizar propuestas técnicas, diseños y documentación.
  - Identificar los problemas y errores antes o cuando se producen.

- Técnico experto en WLAN, LAN y cableado cuyas funciones son:
  - Realizar el despliegue y configuración de toda la arquitectura existente en el despliegue.
  - Realizar el trabajo de campo, en el que se incluyen los replanteos y los estudios de cobertura in situ.
  - Crear los servicios que son ofrecidos a los usuarios.
  - Gestionar las herramientas de monitorización de redes WLAN y LAN.

2 Toma de requisitos

"En la vida siempre es sí, nunca no."

ÁNGEL NARANJO SÁNCHEZ

En este capítulo se contextualizan las características y necesidades con las que cuenta esta sede para posteriormente poder analizarlas y aportar las soluciones óptimas que satisfagan todos los requisitos.

2.1 Especificación de los requisitos

A continuación se exponen y detallan los requisitos, definidos por los responsables de la sede, basados en la idea de que la red esté al servicio de los usuarios y no sean los usuarios los que se adapten al diseño de la red.

De esta forma se distinguen:

- Integrar la red de la sede con la Red Corporativa de la empresa.
- Actualizar la red LAN de la sede debido a la existencia de equipos que se encuentran en condiciones precarias.
- Crear una nueva red de área local inalámbrica (WLAN) que satisfaga las necesidades de cobertura y capacidad contempladas por los responsables de la sede, entre las que se incluye el edificio central del parque y la explanada que se encuentra frente a su fachada exterior.

  Esta necesidad surge a raíz del creciente uso del parque como núcleo de actos sociales y culturales, que requieren el empleo de dispositivos móviles con conexión Wi-Fi tales como portátiles, teléfonos móviles, tabletas o PDAs. En definitiva, dispositivos que son utilizados en las reuniones o eventos, y que necesitan tener una conexión segura, fiable y rápida.
- Conectar la red LAN existente con la nueva WLAN.
- Ofrecer servicio a un máximo de entre 100-110 personas, contando empleados del parque (EMPLEADOS), empleados de otras sedes (ITINERANTES) y visitantes (INVITADOS).
- Dar acceso para los trabajadores y personal laboral del propio parque, separado del servicio ofrecido para los visitantes.
- Reutilizar e integrar el servidor de direccionamiento DHCP propio de la sede con la Red Corporativa de la empresa. En la arquitectura inicial es usado para asignar direccionamiento a todos los equipos físicos conectados a la red LAN, tales como ordenadores de mesa e impresoras.
- Dotar de un acceso controlado para los visitantes mediante una página Web de registro (portal cautivo) que debe aparecer al conectarse a Internet. Esta Web debe ofrecer un formulario donde poder crear una cuenta de usuario INVITADO del parque o poder iniciar sesión con una cuenta ya creada. Las

nuevas cuentas se deben activar a través de un correo enviado a la persona responsable de los mismos que es asignada por la directiva de la sede.

- Limitar la validez de la cuenta de INVITADOS a tres días de duración que es el tiempo medio que tiene cualquier actividad realizada en sus instalaciones.
- Crear un sistema de gestión de los usuarios INVITADOS con una interfaz simple e intuitiva que se encarga de las cuentas nuevas, las ya creadas y las expiradas, con capacidad de crear/borrar masivamente las cuentas.
- Utilizar como fuente de autenticación el Active Directory de la sede, en el que se definen los datos identificativos de cada usuario (nombre, contraseña, MAC y grupo al que pertenece).
- Disponer del servicio en cualquier momento del día sin restricciones en el horario de conexión.
- Ajustar el coste del proyecto al capital del que dispone la sede no superando los 12.000 €.
- Acatar la normativa existente en cuanto a emisiones radioeléctricas y limitaciones de potencia.
- Seguir las especificaciones recogidas en la Orden de 2 de junio de 2017, reguladora de los requisitos necesarios para el diseño e implementación de infraestructuras de cableado estructurado y de red de área local inalámbrica. (BOJA Nº108 D08/06/2017).
- Cumplir la normativa CNMC. (Comisión Nacional de los Mercados y la Competencia).

3 Fase de análisis

"Todo en la vida hay que afrontarlo con valor"

Mª AMELIA CANO GARCÍA

Tras describir los requisitos del cliente, plasmar las necesidades que plantean y delimitar los objetivos técnicos del proyecto, es momento del estudio y análisis de la arquitectura de red existente. En primer lugar se describe la situación geográfica y el entorno donde se sitúa y tras la contextualización se llega a las conclusiones y decisiones que desencadenan en la primera aproximación de la red.

3.1 Análisis sobre el terreno

El proyecto se desarrolla en la sede que gestiona uno de los mayores parques de la ciudad, concretamente en el edificio central de este, lugar principal y más conocido del mismo.

Este centro neurálgico es un edificio compuesto de dos plantas, cada una de ellas cuenta con varias salas donde se realizan actividades culturales y exposiciones. En la planta inferior se encuentra la oficina de gestión del parque, lugar donde los empleados planifican todas las actividades ofrecidas y es el punto de información de los visitantes. Además del edificio central destacan dos edificaciones que lo envuelven, en ellas se sitúa un salón de actos que es reservado durante franjas horarias concretas a colectivos que lo solicitan, una biblioteca y una sala de estudio. El punto de unión de estas estancias reside en el patio central, donde se pueden realizar numerosas citas culturales como teatro, cine, talleres, cócteles...

El patio es la estancia más utilizada y visitada, es el punto inicial de todas las actividades con las que cuenta el parque, tales como:

- Actividades infantiles.
- Actividades de recreación de un yacimiento arqueológico.
- Actividades de restauración.
- Actividades de recreo canino.
- Actividades de huertos ecológicos.
- Piragüismo o kayak.
- Esquí o esquí acuático.

A continuación en la figura Figura 3.1 podemos observar los dos patios, el primero se encuentra entre el edificio principal y las dos edificaciones que lo envuelven y el segundo situado frente a la fachada exterior.

Figura 3.1 Edificio y patios de la sede.

.

3.2 Estado actual

La arquitectura inicial de la sede está compuesta por el cableado estructurado que constituye la red LAN, que interconecta a los equipos fijos de los empleados y les da salida a Internet.

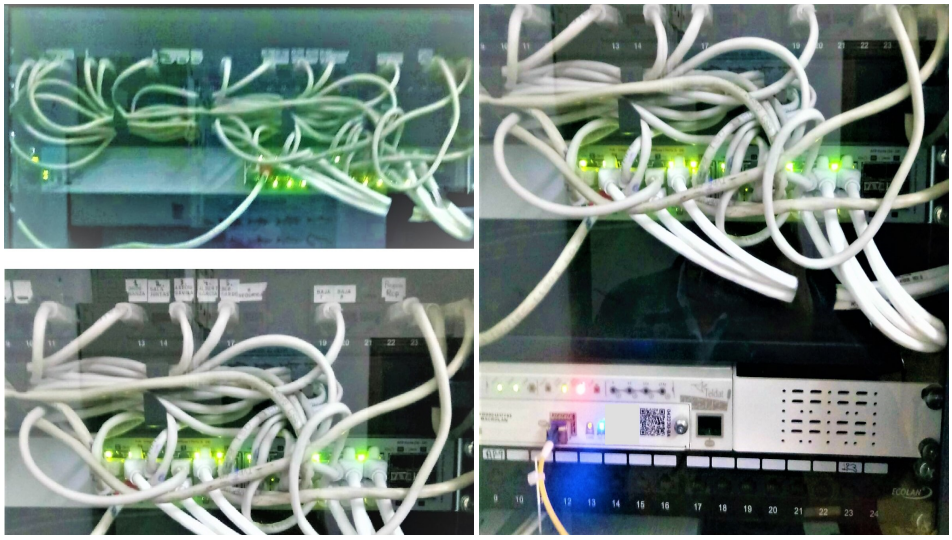
Para poder realizar un análisis más detallado de cada elemento de la arquitectura inicial, se divide en tres bloques fundamentales:

- Cableado estructurado.
- Red de Área Local (LAN).
- Red inalámbrica (WLAN).

En secciones posteriores se explican los elementos que componen cada bloque, analizando las carencias y los elementos que pueden ser reutilizados.

3.3 Sistema de cableado estructurado

El centro de procesamiento de datos (CPD) se encuentra en la planta baja del edificio, en la primera sala de la izquierda (tal y como se observa en la Figura 3.4). Esta estancia es de aproximadamente 12 metros cuadrados, cuenta con un armario de 19" de 9U de la marca GTLAN cuyas dimensiones son: 450x600x52 mm aproximadamente, un panel de parcheo cableado hasta las tomas de red con cable UTP Cat 6, además de un router y un switch. En la Figura 3.2 se observa el estado inicial del armario y del cableado.



(a) Cableado inicial (b) Router y switch

Figura 3.2 Conexiones CPD iniciales.

Todas las conexiones desplegadas en la sede se inician en esta sala. El cableado vertical hacia la primera planta se consigue a través de un pasamuros existente en el techo de esta sala. El cableado horizontal con conexión al edificio contiguo se logra mediante otro pasamuros existente en la pared exterior a través de un tendido aéreo, aportando conectividad al salón de actos y la biblioteca. En la Figura 3.3 podemos observar el pasamuros del edificio principal hacia el exterior y el tendido aéreo entre éste y las edificaciones anexas.

Figura 3.3 Pasamuros hacia exterior y tendido aéreo.

.

El cableado estructurado inicial del edificio se basa en la interconexión de todos los equipos fijos con el armario donde se sitúa el switch y el router. La Figura 3.4 muestra la localización de cada una de las estancias de la planta baja y representa el cableado y los equipos fijos existentes, como último detalle se especifica la ubicación de la vertical por donde se extiende el cableado hasta la planta superior.

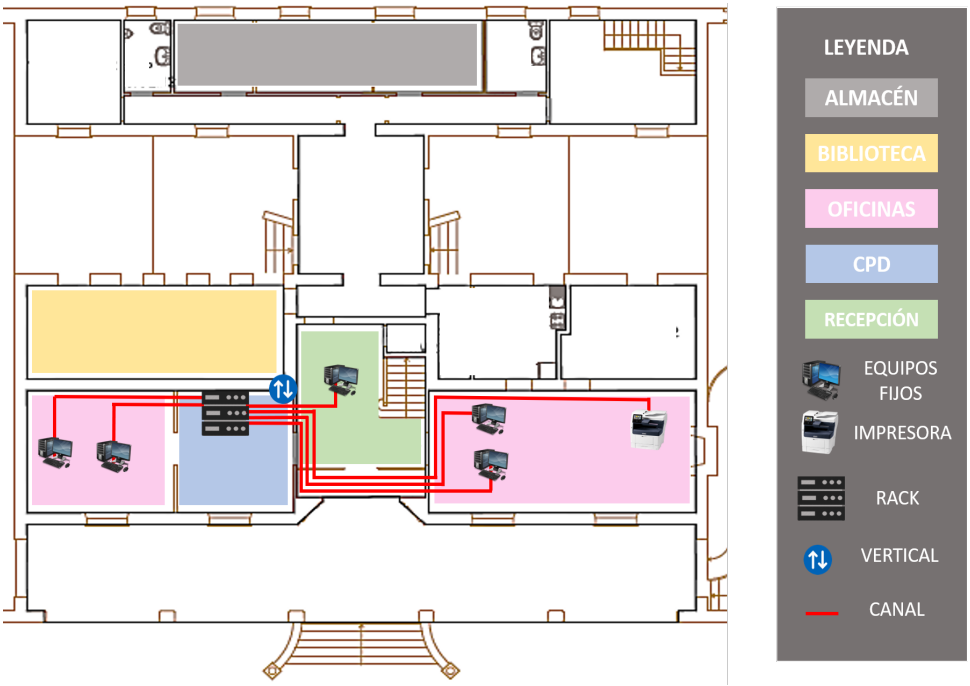


Figura 3.4 Cableado estructurado inicial de la planta baja.

La Figura 3.5 muestra el emplazamiento de cada una de las salas de la primera planta y señala el cableado estructurado que interconecta a los equipos fijos.

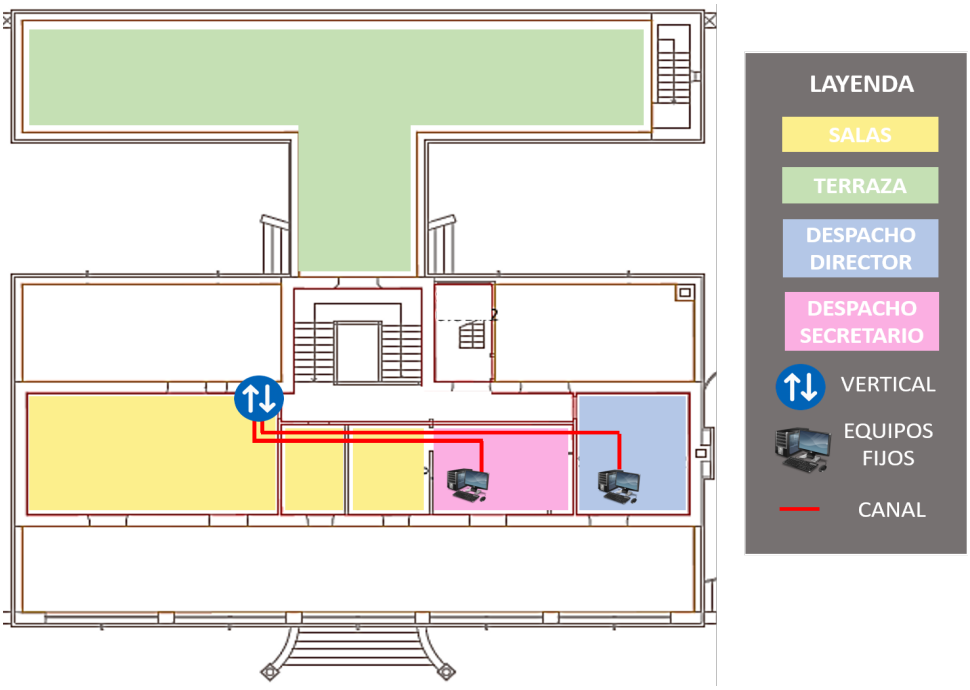


Figura 3.5 Cableado estructurado inicial de la planta primera..

La Figura 3.6 muestra un mapa completo de la sede, compuesta por el edificio central, dos edificaciones anexas y un patio interior. Los detalles que se representan son el emplazamiento del cableado estructurado, el tendido aéreo y los pasamuros que interconecta ambos edificios.

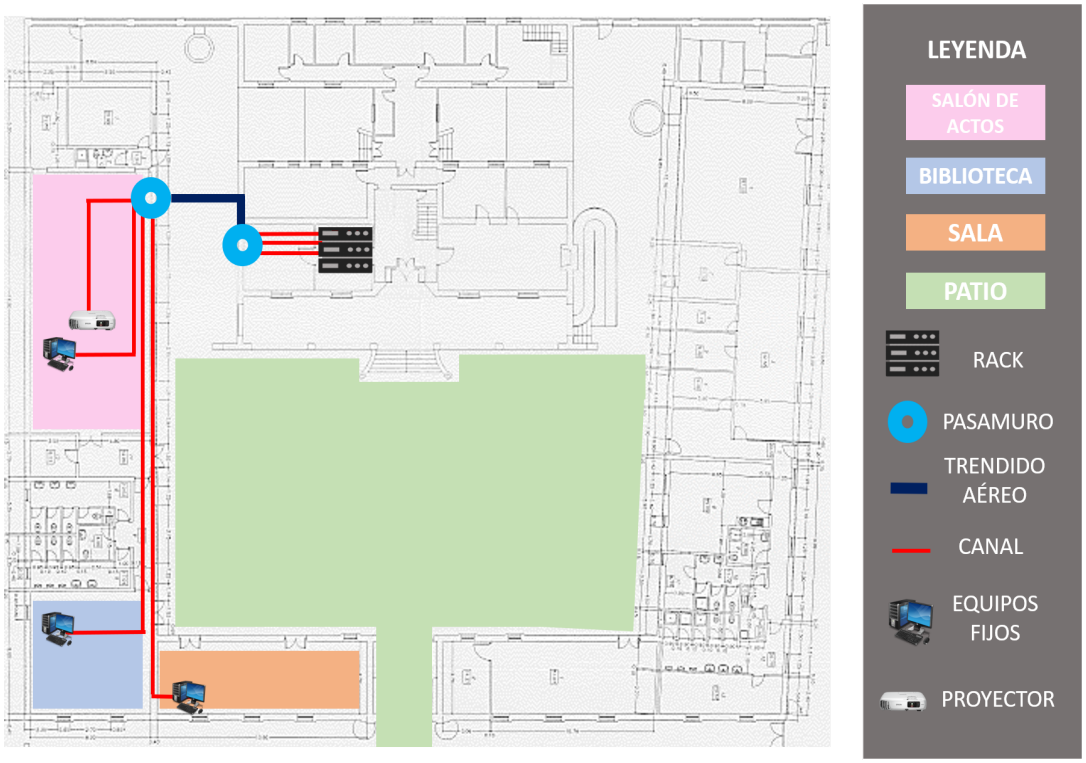


Figura 3.6 Cableado estructurado inicial de la edificación que envuelven al principal.

.

Algunos equipos de trabajo no pueden utilizarse debido a problemas existentes en el cableado estructurado, por lo que surge la necesidad de sustituir el cableado que falla y actualizar la diversidad de categorías. Para conocer los cambios que se necesitan realizar y poder llevar a cabo esta actualización se procede a la ejecución de un análisis y certificación del cableado.

3.3.1 Estudio y análisis de cableado estructurado

El análisis del cableado estructurado se realiza con certificadores de cables de cobre de la serie DTX CableAnalyzer de Fluke Networks, que ejecutan pruebas para garantizar la calidad de los componentes, de la instalación y el cumplimiento del estándar ANSI/TIA/EIA-568-B. Esta norma establece los parámetros a medir, el tiempo de medición, los límites que distinguen el "PASA" del "NO PASA" y los requisitos de los instrumentos de medición de las pruebas de campo.

Cuando se habla de enlace permanente se trata de la instalación cableada fija que va desde la roseta donde se conecta el equipo fijo hasta su correspondiente puerto en el panel de parcheo del CPD. Las pruebas sobre él se realizan utilizando el adaptador DTX-PLA002, con el conexionado que se encuentra en la Figura 3.7.

Los parámetros que se van a certificar son:

- Longitud del cable.

  Esta prueba mide la longitud de cada par del cable, verificando que se encuentra dentro de los límites indicados por la norma. Esta medida es obtenida mediante la velocidad de propagación (NVP) dada por el fabricante.

  El cableado estructurado que se certifica en esta sede es de Cat6, su NVP es de 69 % y la longitud máxima permitida por la norma es 100 metros.

Figura 3.7 Conexionado certificación Fluke.

.

- Retardo de propagación.

  El retardo de propagación se define como el tiempo que tarda la señal en llegar al otro extremo del cable. Esta magnitud es medida en nanosegundos (ns) y en el cableado UTP Cat 6 debe ser menor que 55 ns para un canal de 100 metros.

- Diferencia de retardo de propagación.

  La diferencia entre la velocidad de la señal de transmisión entre el par más rápido y el par más lento es lo que evalúa este parámetro, tal y como muestra la Figura 3.8. Esta magnitud es medida en ns y el cableado UTP Cat 6 debe ser menor que 50 ns para un canal de 100 metros.

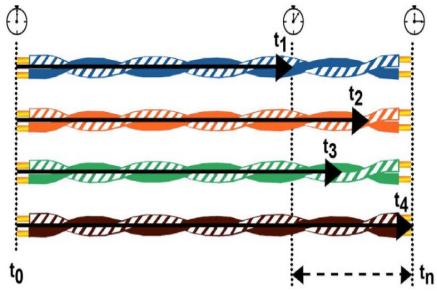


Figura 3.8 Diferencia de retardo de propagación con certificación Fluke.

- Atenuación (pérdida de inserción).

  La atenuación se define como la pérdida de potencia al transmitirse por el cable, cuantifica la resistencia que opone ante las transmisiones. Esta magnitud se expresa en decibelios (dB). Los valores más bajos de la atenuación corresponden a un mejor rendimiento del cable.

  El exceso de longitud del cable es el fallo más común que produce una atenuación superior a los límites permitidos. En la Figura 3.9 se observa un ejemplo del resultado que podemos obtener. La línea roja muestra los límites de la pérdida de inserción según la norma. Los valores de la medición deben estar por debajo de la línea roja, lo que significa que la pérdida es menor que el límite del estándar TIA / ISO.

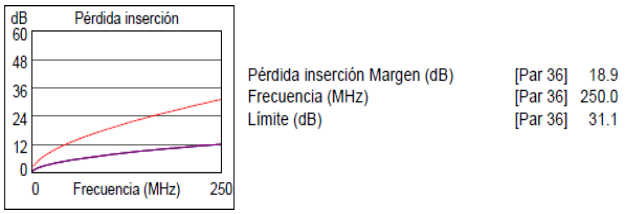


Figura 3.9 Atenuación con certificación Fluke.

- Mapa de cableado.

  Esta evaluación comprueba las conexiones de los ocho conductores entre el extremo lejano (toma de red) y el extremo cercano (panel de parcheo) del cable. Además verifica la continuidad de cada par, el apareamiento y la longitud. Algunos de los errores más comunes de esta prueba se encuentran en la Figura 3.10.

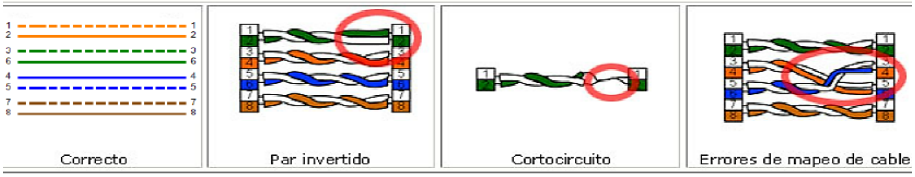


Figura 3.10 Ejemplos de errores de mapa de cableado con certificación Fluke.

- Paradiafonía (NEXT).

  La paradiafonía mide la interferencia que ejerce un par sobre otro en el extremo más cercano. En la Figura 3.11 - (a), la línea roja muestra los límites según la norma y las líneas de colores reflejan las seis combinaciones de pares, siempre que estén por encima de la línea roja, el cable pasará la certificación. Cuanto mayor sea el valor, mejor es el resultado.

- Cociente de atenuación a paradiafonía (ACR-N)

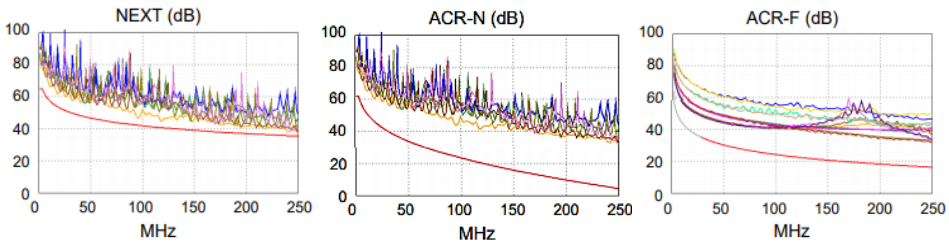
  La prueba ACR-N proporciona los resultados de seis combinaciones (par a par) para un cable de 4 pares, es un calculo no una medida. Se obtiene a partir de la siguiente fórmula y se expresa en dB:

$$ACR_N = NEXT - atenuacion \tag{3.1}$$

- Cociente de atenuación a telediafonía (ACR-F)

  La telediafonía (FEXT) mide la interferencia que ejerce un par sobre otro en el extremo más lejano. La prueba ACR-F realizada en los 4 pares del cable es un calculo que se obtiene a partir de la siguiente fórmula y se expresa en dB:

$$ACR_F = FEXT - atenuacion \tag{3.2}$$



(a) Ejemplo de NEXT (b) Ejemplo de ACR-N (c) Ejemplo de ACR-F

Figura 3.11 Ejemplos de gráficas de NEXT, ACR-N Y ACR-F.

Todas las conexiones de enlace permanente que se comprueban son cables UTP de Cat6 con conexión directa. Durante la prueba se analizan un total de 12 cables de cobre que están desplegados desde el panel de parcheo del CPD hasta cada una de las tomas de red de los equipos fijos que se muestran en la Figura 3.4, la Figura 3.5 y la Figura 3.6.

Tabla 3.1 Resultado certificación cableado estructurado.

Resultado informe	Resultados individuales de las pruebas	Enlaces CAT6
PASA	Pasan todas las pruebas	10
PASA*	Uno o más parámetros pasan marginalmente las pruebas y el resto pasan correctamente	1
FALLA*	Uno o más parámetros fallan marginalmente las pruebas y el resto pasan correctamente	0
FALLA	Uno o más parámetros fallán	1

Fluke avisa cuando el análisis de un cable se encuentra en su zona de incertidumbre mediante un resultado con un asterisco. Un PASA* debe estudiarse para que sea aceptado como un PASA, mientras que un FALLA* debe considerarse como un resultado negativo. En la tabla podemos observar que existen dos cables que deben estudiarse para poder solventar los errores.

El primer cable que se analiza es el que tiene como resultado PASA*, según su informe se debe a no cumplir los niveles establecidos de la norma respecto a la pérdida de retorno.

El segundo cable que se analiza es el que tiene como resultado FALLA, se debe a un cortocircuito como nos muestra la prueba de mapeo de cables, el cable se encuentra dañado y necesita ser sustituido.

Tras analizar todos los enlaces permanentes, se estudian todos los latiguillos que componen los canales que se sitúan entre la toma de red y el equipo de trabajo, así como, entre el panel de parcheo y los equipos de interconexión. Al finalizar el estudio se descubre que algunos de ellos son de Cat6 y otros de Cat5e lo que provoca que la categoría del canal final descienda al elemento de menor categoría.

3.4 LAN

3.4.1 Red Corporativa

La Red Corporativa de la empresa proporciona altas capacidades en cuanto a seguridad, control del tráfico, control del direccionamiento y redundancia, así como, una gestión y autenticación centralizada que garantiza un alto nivel de rendimiento.

Existe un Nodo Central donde se encuentran físicamente instalados los equipos que hacen posible el funcionamiento centralizado de toda la arquitectura, tales como el servidor DHCP, la controladora master o las terminadores de túneles además del servidor de autenticación y monitorización.

A continuación en la Figura 3.12 se observa el esquema de los elementos que la componen y que son explicados a continuación.

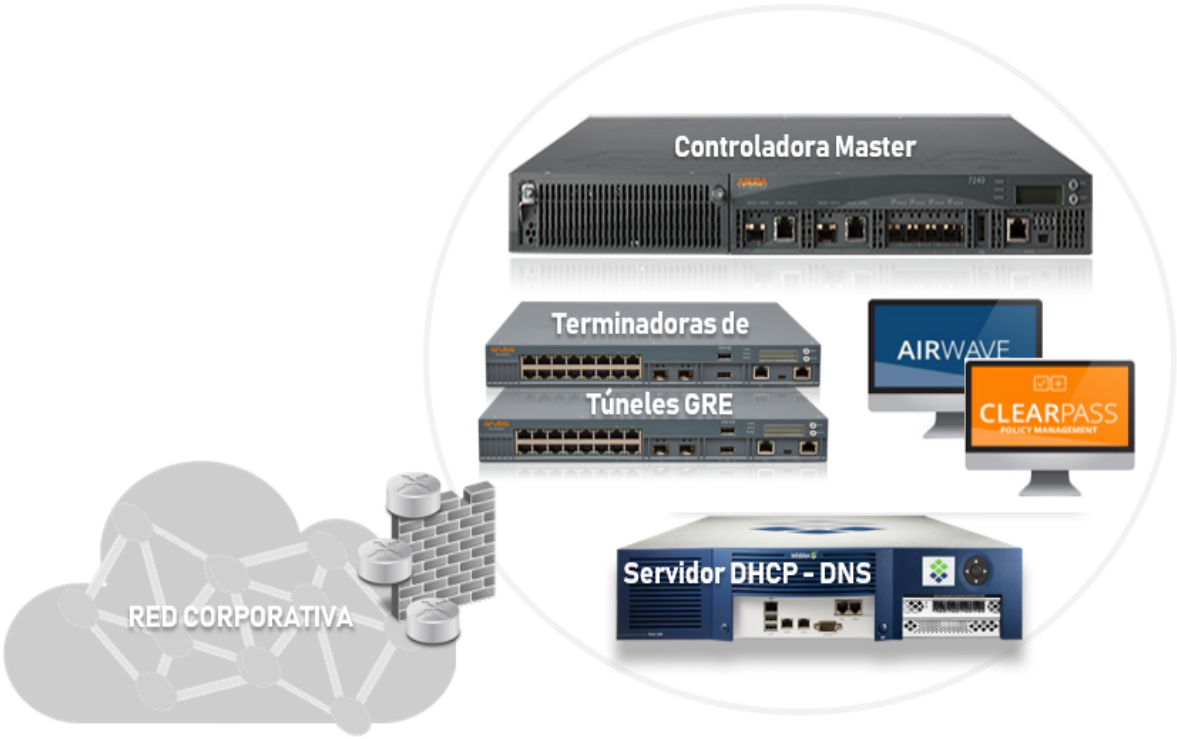


Figura 3.12 Elementos de la Red Corporativa.

.

3.4.1.1 Servidor DHCP

El servidor de direccionamiento centralizado ofrece la administración integrada de DNS y direcciones IP para los empleados de otras sedes de la empresa (ITINERANTES) y a los visitantes del parque (INVITADOS).

3.4.1.2 Controladora master

La controladora master es la que actúa como núcleo de la Red Corporativa, administra servicios de autenticación, encriptación, conexiones VPN, análisis de espectro, protección contra intrusiones inalámbricas y es el servidor de licencias, lo que hace aun más centralizada la red.

3.4.1.3 Controladoras terminadoras de túneles

Existen dos terminadoras de túneles que están configuradas a modo de clúster para que funcionen como una única entidad lógica y tienen la capacidad de soportar la caída del controlador local de cualquier sede de la empresa. Actúan como punto de terminación de los túneles GRE que prestan servicio a los usuarios ITINERANTES e INVITADOS cuyo tráfico es tunelizado desde la sede hasta este punto para poder gestionarlo y administrarlo correctamente.

3.4.1.4 Servidor de autenticación y control de acceso

El servidor de autenticación y control de acceso se compone de varios módulos, asociándose cada uno a un tipo de servicio. El módulo central, Policy Manager, es el servidor AAA, pudiendo utilizar para ello el protocolo RADIUS. El segundo módulo, Guest, es el servidor para los usuarios INVITADOS, que permite su provisión de manera sencilla y segura.

Otra característica a destacar es la posibilidad de utilizar una gran variedad de fuentes de autenticación, LDAP, AD, o SQL. Sobre ese módulo central se asientan el resto de servicios, como son OnGuard (permite obtener información adicional de los clientes conectados a la red) y OnBoard (gestiona los dispositivos móviles).

3.4.1.5 Sistema de monitorización

El módulo de monitorización ofrece una vista detallada de todas las redes cableadas e inalámbricas que existen. Monitoriza de manera proactiva el tiempo que tarda un dispositivo móvil en asociarse, en autenticarse en un servidor RADIUS, en recuperar una dirección IP a través de DHCP o en resolver nombres para los servicios DNS. Proporciona claridad y control en toda la red a través de monitoreo en tiempo real e informes históricos.

3.4.2 Red de la sede

La arquitectura que compone la red LAN inicial es simple aunque cuenta con equipos de grandes capacidades. Existe un router con el que tienen acceso a Internet, un servidor de DHCP que da direccionamiento a los equipos fijos con los que trabajan los empleados y un switch al que se conectan todos estos equipos de trabajo, impresoras y un proyector.

Con idea de poder reutilizar cualquier equipo a la hora de realizar el diseño final de la red, se analizan las características de cada componente.

El router con el que cuenta es el modelo Teldat-M1, compacto de 1U y sin ventiladores, para no generar ruido por lo que es adecuado para oficinas. Una de las características imprescindibles es la escalabilidad ya que cuenta con hasta 500 Mbps con servicios activos y un slot para adaptarse a distintos entornos (fibra, ADSL/VDSL, G.SHDSL, E1/T1, serie, conmutador Ethernet PoE) lo que lo hace manejable y reutilizable. Otra propiedad relevante es la conectividad con la que cuenta ya que tiene cuatro puertos Ethernet 10/100/1000 con funcionalidades VLAN, 802.1P/Q/X. En este caso solo es de utilidad uno de ellos para conectarlo con el switch.

En el caso del switch, disponen de un conmutadores HP 2530. Cuenta con 24 puertos RJ-45 10/100/1000 y cuatro ranuras SFP para conectividad de fibra. Permiten Power over Ethernet para implementaciones de voz, video o inalámbricas.

El servidor DHCP es una maquina Linux con el software Dnsmasq. Este actúa como servidor de direcciones IP para los equipos de usuarios que se conectan a nivel físico a la LAN.

3.5 WLAN

Para complementar la red existente y dar servicio a los distintos dispositivos móviles existe la necesidad de instalar una red de área local inalámbrica. Como punto inicial en el desarrollo de la red WLAN se lleva a cabo un estudio de cobertura teórico que permite conocer el alcance y la cobertura de los puntos de acceso para poder decidir la ubicación preferible para ellos.

3.5.1 Estudio de cobertura teórico

El estudio de cobertura teórico es realizado en las dos plantas del edificio principal así como en las edificaciones donde se encuentran el salón de actos, la sala de estudio y la biblioteca. El criterio con el que se posicionan los puntos de acceso es el poder conseguir la señal más óptima en todas las zonas, con el menor número de ellos.

A partir de ahora en el proyecto consideraremos una señal óptima en la horquilla de 70-50dbm. En el estudio se han incluido tres puntos de acceso para exteriores con el fin de dar cobertura a los dos patios.

Tabla 3.2 Resumen de APs por planta.

Nuevo equipamiento	
Planta	Propuesta de instalación
Planta principal	4
Planta primera	2
Anexo y exterior	3
TOTAL	**9**

Este primer estudio de cobertura teórico se realiza con AirMagnet Planner, simula los puntos de acceso y las características de la antena y del edificio para predecir la cantidad de puntos de acceso que se necesitan y sus ubicaciones respectivas antes de una implementación Wi-Fi real.

También proporciona información detallada para los puntos de acceso desplegados:

- Nombre / dirección MAC del punto de acceso.
- Canal / SSID asignado.
- Coordenadas de ubicación planificadas para el punto de acceso.
- Altura del punto de acceso / antena sobre el nivel del piso.
- Tipo de antena y sus especificaciones.

La Figura 3.13, Figura 3.14 y Figura 3.15 muestran la cobertura de la señal (en dBm) en cada punto del diseño del mapa. Como regla general, las regiones con intensidades de señal por debajo de -70 dBm proporcionan una cobertura insuficiente para el uso estándar (este valor puede variar según los requisitos del usuario, los acuerdos de nivel de servicio, las aplicaciones utilizadas, el número de usuarios atendidos, etc.).

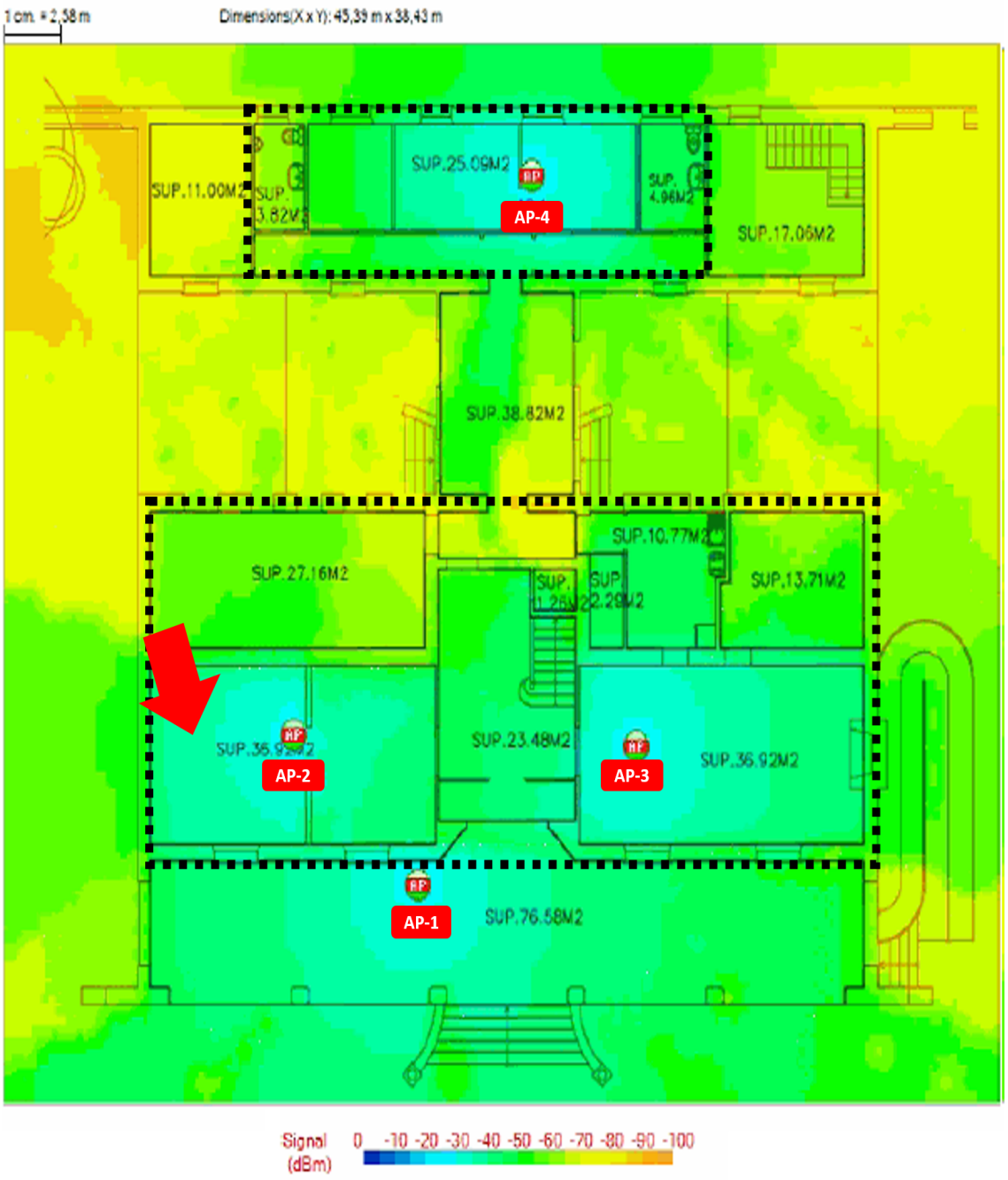


Figura 3.13 Cobertura planta principal.

.

La Figura 3.13 muestra la planta baja donde se encuentra la recepción del edificio bajo las escaleras principales frente a la puerta de entrada, además cuenta con dos salas destinadas al personal de la sede. A la izquierda junto a la puerta principal está el CPD. En la parte posterior del edificio se hallan un par de salas, baños y escaleras. En esta planta se ha dado prioridad a las zonas sombreadas en color negro ya que es donde se ubican los empleados y necesitan la mejor cobertura para poder trabajar en las mejores condiciones.

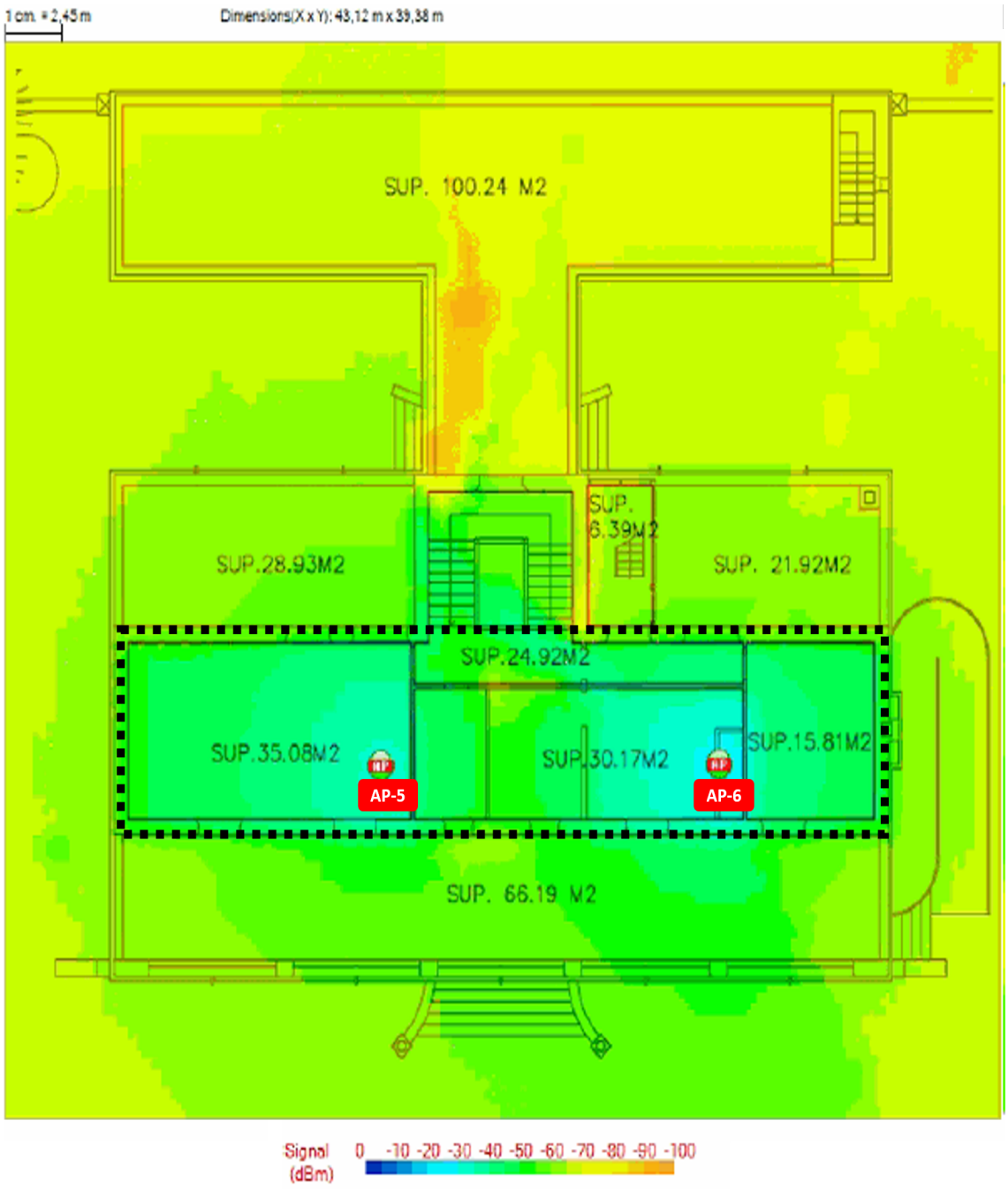


Figura 3.14 Cobertura planta superior.

.

La Figura 3.14 presenta la planta superior dedicada a exposiciones y demás eventos culturales para los que la empresa ofrece sus instalaciones. En esta planta se ha dado prioridad a aportar la mayor cobertura a la zona que se encuentra subrayada en color negro. En el espacio de escaleras y pasillo la cobertura es menos relevante.

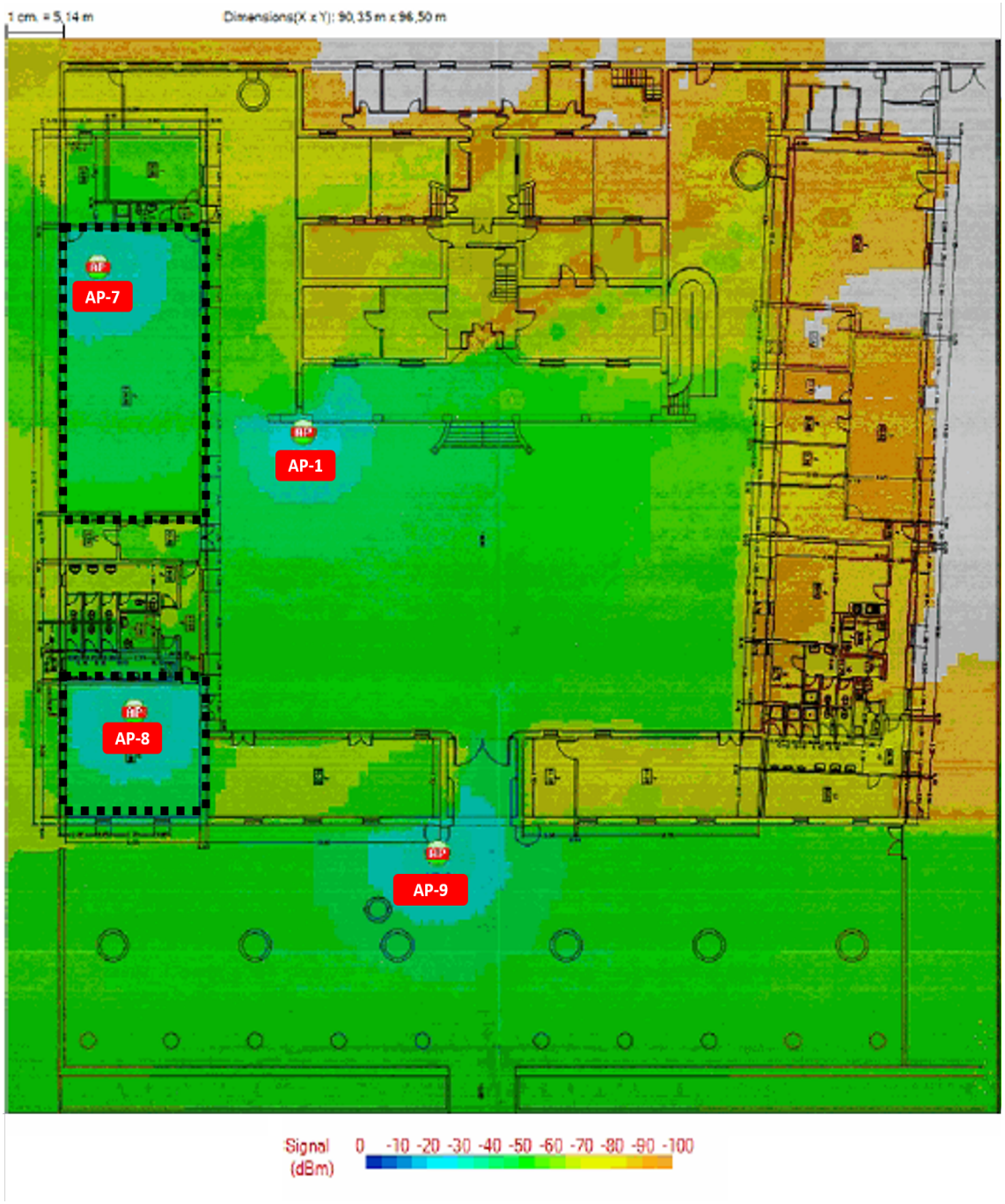


Figura 3.15 Cobertura salón de actos y biblioteca.

.

La Figura 3.15 representa los edificios anexos donde se encuentran el salón de actos y la biblioteca. Entre el edificio principal y el anexo se sitúa el patio interior y tras la fachada principal del edificio se sitúa el patio exterior.

3.6 Estimación técnica inicial

Tras el previo estudio que se ha llevado a cabo se toman las decisiones que se desarrollan a continuación divididas por bloques:

3.6.1 Cableado Estructurado

- **Sustitución de los enlaces permanentes que han obtenido en el análisis FALLA y PASA***

  El enlace permanente con resultado FALLA debe ser sustituido ya que no cumple con la norma mientras que el enlace permanente con resultado PASA* es estudiado para intentar solucionar el problema. El fallo está en las pérdidas de retorno, lo que puede deberse a un fallo en su instalación que pudo ocasionar un destrenzado del cable o deformaciones en él. Como medida preventiva y para asegurar una conexión eficiente se toma la decisión de sustituir también este enlace permanente. La conclusión a la que se llega es la sustitución de ambos enlaces a Cat6A.

- **Sustitución de tomas de red**

  Aquellas tomas de red de los enlaces permanentes que se sustituyen son renovadas para poder aportar las mejores prestaciones y que no supongan un cuello de botella para las nuevas instalaciones.

- **Sustitución de latiguillos**

  Los latiguillos son los responsables del empeoramiento de la calidad del canal al bajar su rendimiento a propiedades de Cat5e. La decisión que se toma radica en la sustitución de todos estos latiguillos a Cat6A. Se elige esta categoría para que en posibles modificaciones futuras el cableado estructurado se pueda alcanzar la máxima velocidad.

- **Etiquetado del cableado**

  Una vez instalados tantos los nuevos latiguillos como los enlaces permanentes que se requieren, se etiquetan con el origen y el destino de la siguiente forma:

  – Orig: Panel de parcheo
    Dest: Toma de red

  – Orig: Toma de red
    Dest: Equipo final

  – Orig: Panel de parcheo
    Dest: Switch

  – Orig: Switch
    Dest: Router

- **Orden, mantenimiento y peinado de cableado**

  Tras la primera supervisión de los cables se observa un desorden generalizado lo que dificulta cualquier tipo de modificación sobre ellos en caso de fallo. La decisión que se toma es reordenar todo el cableado que así lo requiera.

3.6.2 LAN

El estudio de la red LAN desemboca en la decisión de reutilizar todos los elementos de red con los que cuentan ya que a nivel funcional cumplen con las necesidades establecidas, además su reutilización no supone corte alguno en el servicio. También pone de manifiesto la inexistencia de VLANs pues todos los dispositivos se encuentran en una red plana donde el direccionamiento es fijo para cada equipo final y es dado por un servidor DHCP que se encuentra en sus instalaciones.

Surge la necesidad de fragmentación y segmentación de la red de forma correcta y ordenada mediante el uso de VLANs lo que aporta mayor seguridad y mejor rendimiento. Tendremos una VLAN para el control de los puntos de acceso, otra para los equipos fijos y otra para la conmutación local de los empleados que se conecten al servicio Wi-Fi. Los usuarios ITINERANTES e INVITADOS no pertenecen a ninguna VLAN a nivel local sino que son tunelizados a nivel 2 mediante un túnel GRE hasta la terminadora de túneles donde se procesa todo el tráfico.

3.6.3 WLAN

Tras el estudio de cobertura que se ha realizado se llega a la conclusión de que la red inalámbrica que se necesita.

Conlusiones tras análisis

Para esta instalación se requieren los siguientes elementos según se ha observado:

- Latiguillos Cat6A
- Nuevo panel de parcheo
- Canalizaciones
- Puntos de acceso con las siguientes características o elementos:
  - Antenas omnidireccionales
    Son aquellas antenas que radian en todas direcciones, lo que facilita la tarea a la hora del despliegue de los puntos de acceso.
  - Múltiple SSID
    Esta característica permite configurar múltiples SSIDs donde cada uno de ellos puede utilizar diferentes métodos de autenticación. Esta propiedad es necesaria para poder incorporar un SSID para los empleados y otro para los usuarios visitantes.
  - Trabajar en 2 canales
    Utilizar un estandar que soporte la tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.
  - Alimentación PoE
    El AP debe permitir alimentación a través de Ethernet lo que facilita el despliegue y la infraestructura de los mismos, esto conlleva una reducción del coste tanto en mano de obra como en cableado e infraestructura.
  - Gestión de radiofrencuencia
    El punto de acceso debe permitir recopilar y gestionar datos de interés sobre el espectro de radiofrecuencia para su posterior explotación a fin de mejorar las prestaciones que ofrece(canal utilizado, banda...)
  - Mínimo 40 usuarios concurrentes
    El punto de acceso debe soportar un mínimo de 40 usuarios conectados al mismo tiempo.
  - Gestión SNMP
    Esta característica debe estar disponible en los puntos de acceso seleccionados para que puedan ser monitorizados desde el núcleo central de la Red Corporativa y puedan ser gestionados por el servidor que existe para ello.

Tras entregar el primer informe con el diseño inicial del cableado estructurado, la red LAN y WLAN, los responsables de la sede deben aceptar esta primera aproximación de la oferta, tanto económica como técnica, para poder continuar con la parte de diseño.

4 Diseño de la red

"Si vas a hacer algo, hazlo bien"

ANTONIO JESÚS CANO GARCÍA

Este capítulo describe el diseño físico y lógico de la red basándose en estudios previos tanto en el bloque de LAN y WLAN como en el bloque de cableado estructurado. Algunos de los estudios que se realizan en el bloque LAN y WLAN son el replanteo planta por planta, el análisis del equipamiento existente en el mercado y la posterior elección y compra. En el bloque de cableado estructurado es el estudio de la cantidad de cables necesarios por nuevo despliegue y la cantidad de ellos que deben ser sustituidos.

4.1 LAN y WLAN

4.1.1 Replanteo

Tras la visualización del diseño inicial los responsables de la sede reflejan nuevas necesidades y peticiones respecto a la coberturas en zonas determinadas, número de puntos de acceso o localización de los mismos. Esto desemboca en la realización de un replanteo in situ para comprobar la viabilidad del estudio de cobertura teórico previo junto con las nuevas peticiones propuestas. Durante el replanteo se recorren las dos plantas del edificio analizando su estructura buscando la ubicación óptima de los puntos de acceso. A continuación se recogen los resultados obtenidos en el análisis por planta:

- **Planta baja**

  El punto de acceso exterior (AP-1) es desplazado, tal y como se muestra en la Figura 4.1 a causa de dos motivos. El primero, poder aportar mejor cobertura al patio interior y al porche de arcos del edificio. El segundo, la puerta principal cuenta con un mosaico de azulejo, lo que supone una gran pérdida de potencia. Por ello no es el lugar óptimo para instalar un punto de acceso.

Figura 4.1 Ubicación final AP-1.

El punto de acceso (AP-2) es desplazado a la sala contigua respecto a la localización del estudio previo y dará cobertura a ambas salas. Ésta modificación se realiza a petición de los responsables de la sede ya que dicha sala es el lugar donde trabajan diariamente los empleados de la sede.

El punto de acceso (AP-3) es desplazado a la puerta principal para poder dar cobertura al pasillo, a la sala de trabajo y demás estancias contiguas. Además la recepción del parque se sitúa frente a la puerta, bajo las escaleras.

El punto de acceso (AP-4) mantiene la posición en la que se sitúa en el estudio de cobertura teórico para dar cobertura a las tres estancias que se encuentran a su alrededor.

Para poder comprobar que las nuevas ubicaciones de los puntos de acceso son la correcta se realiza un nuevo estudio de cobertura. En la Figura 4.2 se plasma la potencia radiada por los puntos de acceso tras el replanteo.

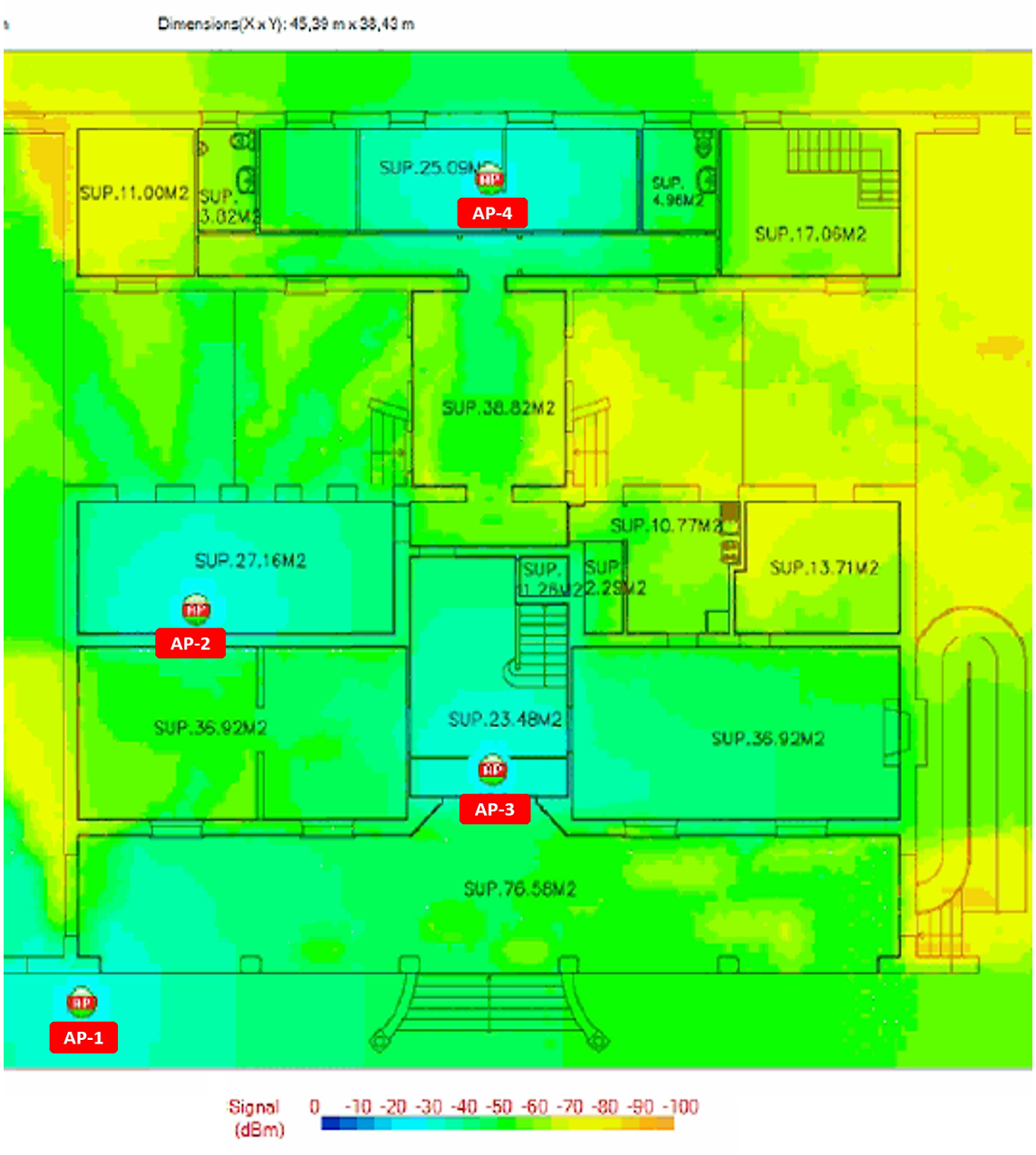


Figura 4.2 Cobertura planta baja.

La Figura 4.3 muestra el nivel de interferencia (en porcentaje) en cada punto del diseño del mapa. Los puntos de acceso se sitúan en las ubicaciones finales y reflejan la potencia especificada. En esta planta se observan altos niveles de interferencia ya que los puntos de acceso se encuentran mas cercanos unos a otros que en el resto de plantas lo que permite saber en que puntos de acceso se tiene que forzar el radiar en un canal particular o tener activo la propiedad ARM.

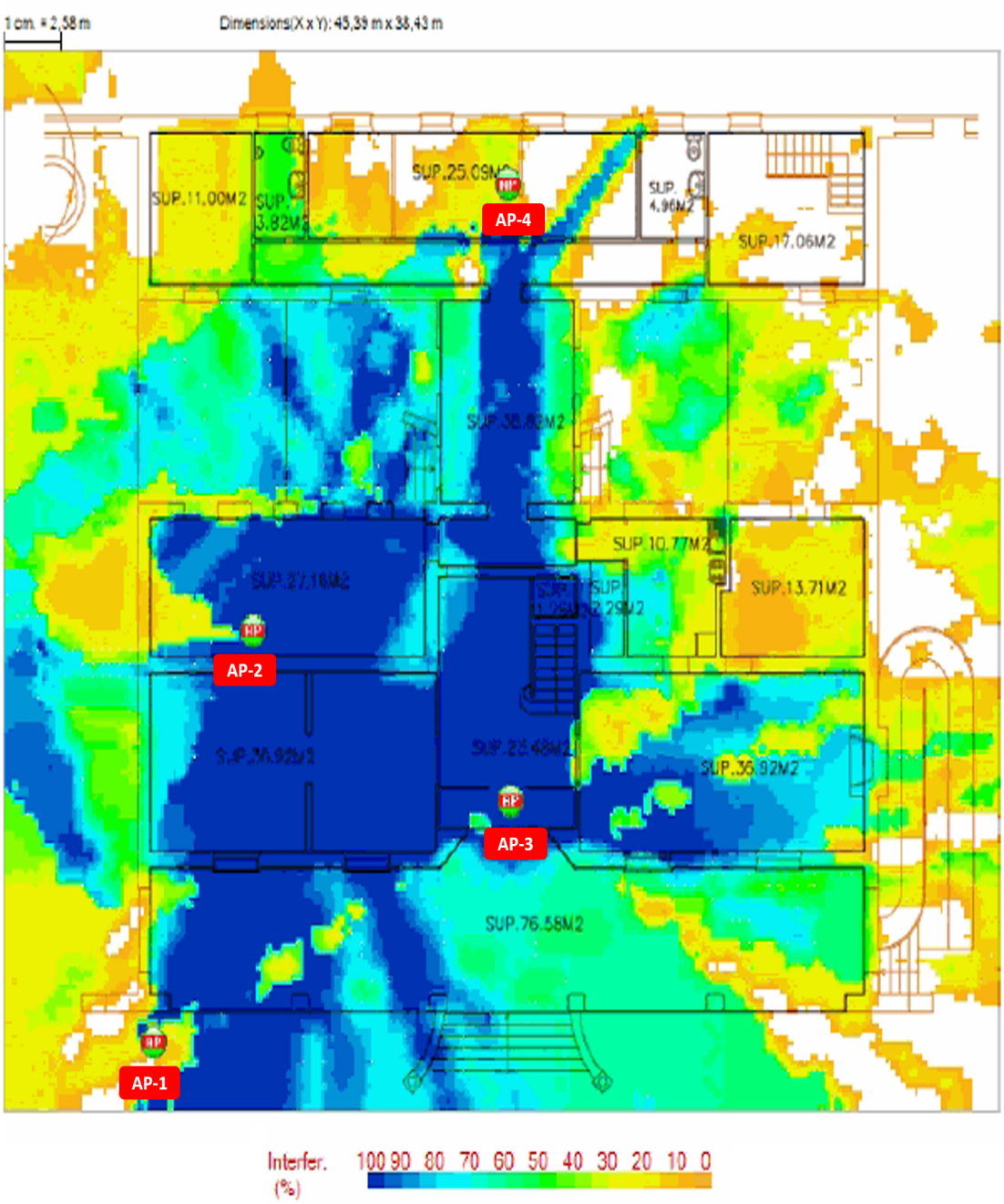


Figura 4.3 Cobertura planta baja.

- **Planta primera**

  Los puntos de acceso que se encuentran en la primera planta (AP-5 y AP-6) mantienen la misma posición que en el estudio teórico inicial y dan cobertura a las estancias interiores de esta planta. Por exigencia de los responsables se planea la instalación de un nuevo punto de acceso exterior para dar cobertura a la azotea de esta planta tal y como muestra la Figura 4.4.

Figura 4.4 Ubicación final AP-7.

En la Figura 4.5 se observa la potencia que es radiada por los tres puntos de acceso.

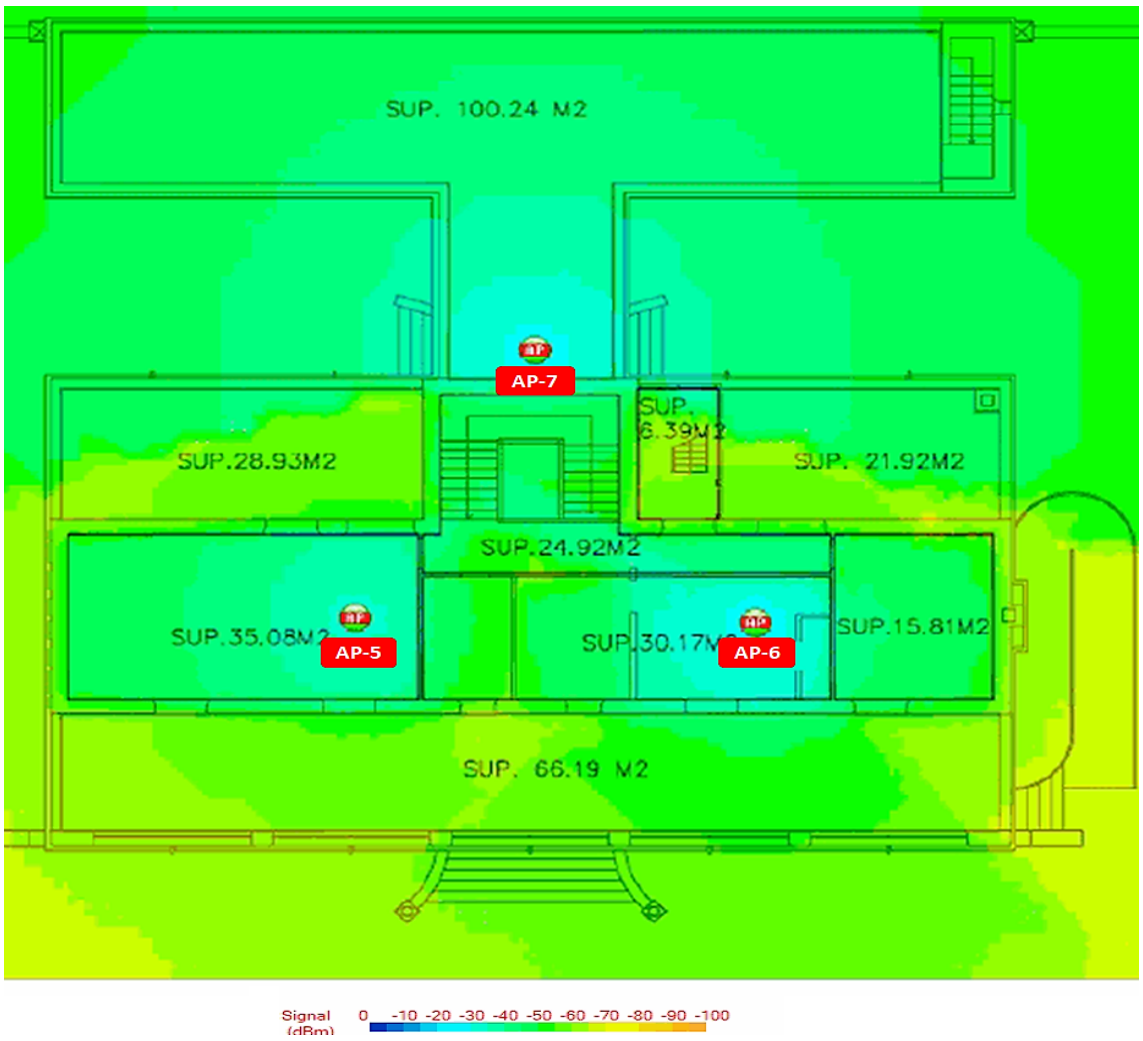


Figura 4.5 Cobertura planta primera.

En la Figura 4.6 se observa el nivel de interferencia existentes en esta planta con la localización final de los puntos de acceso. Los niveles son muy elevados en la unión de los tres puntos de acceso aunque se tiene en cuenta que los niveles de interferencia presentes en el entorno pueden variar dependiendo de varios factores, como la cantidad de AP en un solo canal, el número de dispositivos presentes, los que no interfieren con 802.11, etc.

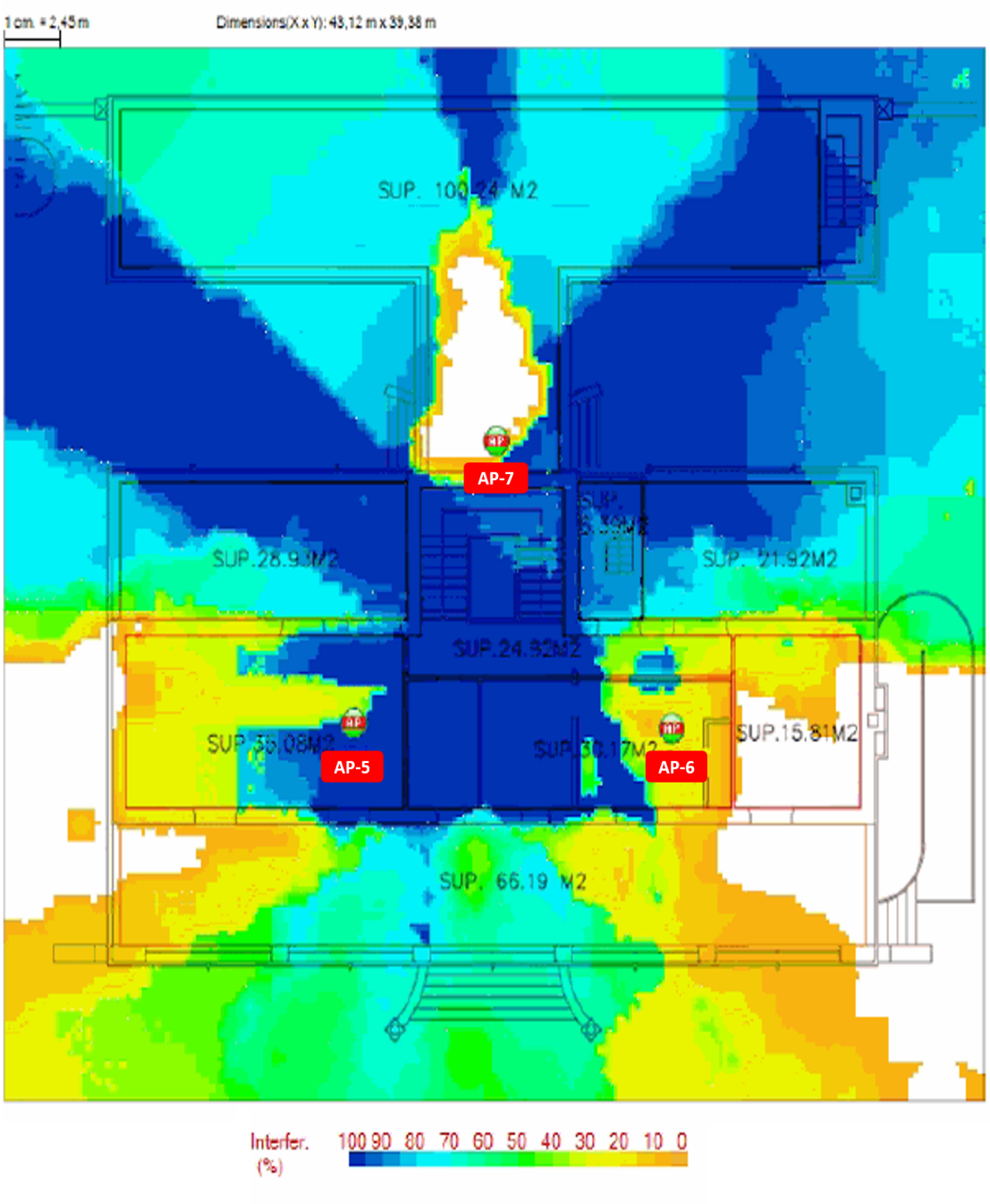


Figura 4.6 Cobertura planta primera.

- **Salón de actos, biblioteca y sala de exposiciones**

  El punto de acceso del salón de actos (AP-8) es retranqueado hasta el centro de la estancia aportando potencia uniformemente a toda la sala aprovechando la canalización del proyector.

  El punto de acceso de la biblioteca (AP-9) mantiene su posición y se añade un punto de acceso (AP-10) a la sala de exposiciones por exigencia de los responsables.

(a) Ubicación final AP-8

(b) Ubicación final AP-9

(c) Ubicación final AP-10

Figura 4.7 Ubicaciones AP-8, AP-9 y AP-10.

El punto de acceso exterior situado encima del arco de la puerta principal se intercambia por dos puntos de acceso colocados en los extremos de la fachada exterior. Esta modificación se produce tras supervisar su arquitectura y diseño, observando que la altura de los extemos es mayor que la de la puerta, lo que mejorará la cobertura.

Figura 4.8 Ubicación final AP-11 y AP-12.

En la Figura 4.9 se puede observar la cobertura en los edificios anexos, en el patio interior y el patio exterior, cumpliendo los requisitos exigidos. Este estudio de cobertura también muestra la incorporación de los nuevos puntos de acceso tanto el exterior para la fachada como el interior para la sala de estudio. El AP-1 se ha incorporado en este estudio para tener una visión total de la cobertura que existe en ambos patios.

Figura 4.9 Cobertura salón de actos y biblioteca.

.

En la Figura 4.10 se observan altos niveles de interferencia en la localización izquierda del plano, esto es debido a que se encuentran tres puntos de acceso relativamente juntos. No existe problema con este hecho, pues como hemos comentado en las anteriores páginas se deberá habilitar ARM en todos estos puntos de acceso.

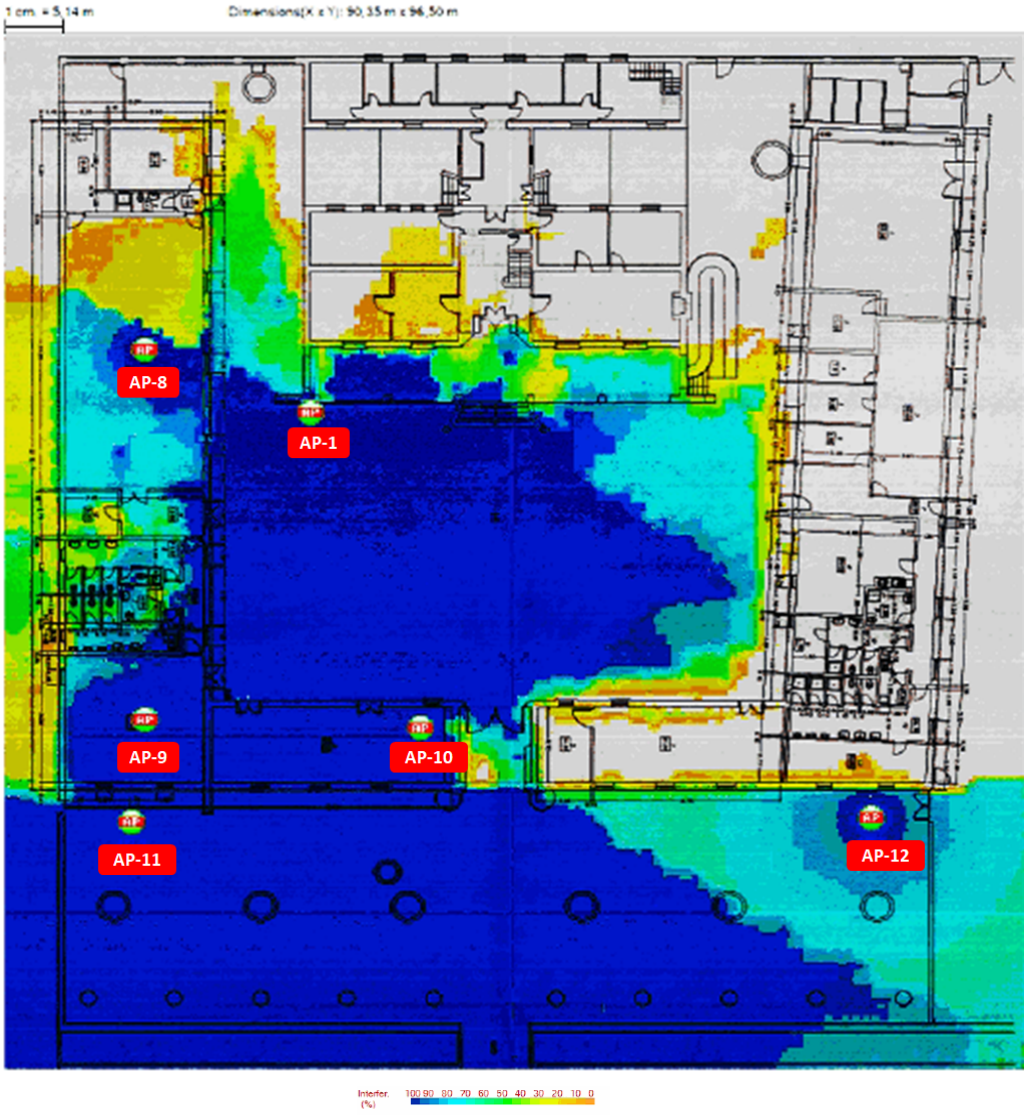


Figura 4.10 Cobertura planta principal.

Conlusiones tras replanteo y nuevo estudio de cobertura

- El número total de puntos de acceso requerido es doce de los cuales cuatro serán exteriores y el resto interiores.
- Incluir un nuevo punto de acceso exterior en la planta primera para que puedan tener cobertura en la terraza trasera.
- Incluir un nuevo punto de acceso exterior para mejorar la cobertura en el patio exterior.
- Mejorar la cobertura tanto en la biblioteca como en la sala de exposiciones que se encuentran en las edificaciones que envuelven la sede.
- En dos de los puntos de acceso se colocan las canalizaciones por el falso techo desmontable. El resto se sacarán directamente del CPD situado en la planta baja teniendo en cuenta que seis de ellos se añadirán utilizando el tendido aéreo existente entre el edificio principal y las edificación que lo envuelve.

4.1.2 Equipamiento

4.1.2.1 Puntos de acceso

La red de acceso contará con puntos de acceso Wi-Fi que deben cumplir cada uno de los requisitos y características que se han mostrado en capítulos anteriores. Para la elección de ellos se ha querido tomar de referencia el Cuadrante Mágico de Gartner y seleccionar las dos empresas más competitivas.

Figura 4.11 Cuadrante mágico de Gartner.

Esta Figura 4.11 está formado por dos ejes, el eje X y el eje Y:

- En el eje X, Gartner define la categoría “completeness of vision” o “visión empresarial” y representa el conocimiento de los proveedores sobre cómo se puede aprovechar el momento actual del mercado para generar valor, tanto para sus clientes como para ellos mismos.
- En el eje Y se encuentra la “capacidad de ejecutar”, que mide la habilidad de los proveedores para ejecutar con éxito su particular visión del mercado.

Ambas divisiones fragmentan el cuadrante en cuatro sectores. Ahí es donde se plasman las principales compañías de cada competencia en función de su tipología y la de sus productos: líderes (leaders), retadores o aspirantes (challengers), visionarios (visionaries) y operador minoritario (niche players).

La evaluación del cuadrante mágico de Gartner se basa en dos criterios: la integridad de visión y la capacidad de ejecución de las compañías. Como resultado se observa que Aruba HP y Cisco se consolidan como empresas punteras en el mundo de las infraestructuras LAN/WLAN, por lo que se analizan ambas.

4.1.2.2 Puntos de acceso de interior

Las características de los distintos dispositivos con los que cuenta **Cisco** que cumplen los requisitos establecidos son:

- Serie 100(AP-131 y AP-150)
  - AP-131 proporciona conectividad 802.11n para clientes a 2,4 GHz y 5 GHz. Compatibilidad con radios de doble banda simultáneas de hasta 300 Mbps por radio.
  - AP-150 proporciona conectividad 802.11ac con velocidad de hasta 1.2 Gbps.
  - Ambos cuentan con antenas internas incorporadas con orientación vertical.
  - Precio bajo AP-131(395 euros) y AP-150(465 euros).

- Serie 300 (AP-351 y AP-361)
  - AP-351 proporciona conectividad 802.11n rentable para clientes a 2,4 GHz y 5 GHz. Admite radios de doble banda simultáneas con un máximo de 300 Mbps por radio.
  - AP-361 proporciona conectividad 802.11ac rentable con velocidad de hasta 1.2 Gbps. Velocidad máxima de datos simultáneos de hasta 867 Mbps en una radio de 5.0 Ghz y 300 Mbps en una radio de 2.4 Ghz.
  - Ambos cuentan con antenas fijas internas e integradas.
  - Precio bajo AP-351(480 euros) y AP-361(535 euros).

    El AP-371 también cumple las necesidades requeridas aunque tiene mayor velocidad y capacidad el precio es mucho más elevado comparando calidad-precio.

- Serie 550/560 (AP-561 y AP-571)
  - AP-561 proporciona conectividad 802.11ac con velocidad de hasta 1.2 Gbps. Velocidad máxima de datos simultáneos de hasta 867 Mbps en una radio de 5.0 Ghz y 300 Mbps en una radio de 2.4 Ghz.
  - AP-571 soporta hasta 1.3 Mbps en una radio de 5.0 Ghz, y 600 Mbps en una radio de 2.4 Ghz.
  - Cuatro antenas (AP-571) y diez antenas (AP-561) fijas internas e integradas.
  - Precio alto AP-561(895 euros) y AP-571(960 euros).

De los anteriores modelos todos cumplen las siguientes características:

- Máximo de 128 conexiones por radio.
- Alimentación directa de CC y alimentación a través de Ethernet (PoE).
- Número máximo de SSID es 16.
- 2x2 MIMO en 5.0 GHz y 2.4 GHz.

Las características de los distintos dispositivos con los que cuenta **Aruba HP** que cumplen los requisitos establecidos son:

- Serie 200 (AP-204 y AP-205)
  - Velocidades de datos inalámbricas de hasta 867 Mbps para tecnología 802.11ac.
  - Cuatro antenas omnidireccionales de doble blanda (AP-204), dos conectores RP-SMA para antenas de banda dual externas(AP-205).
  - Precio medio (695 euros).

- Serie 207
  - Velocidad máxima de datos simultáneos de 867 Mbps en la banda de 5 GHz y 400 Mbps en la banda de 2,4 GHz.
  - Permite servicios basados en ubicación con dispositivos móviles con BLE.
  - Dos antenas omnidireccionales de inclinación.
  - Precio bajo (343 euros).

- Serie 210
  - Velocidades de datos de hasta 1.3 Gbps a dispositivos de 5 GHz con tecnología 802.11ac
  - Seis antenas integradas omnidireccionales (AP-214) y tres conectores de antena RP-SMA externos combinados y dúplex (de doble banda) (AP-215).
  - Precio elevado (995 euros).

- Serie 220
  - Velocidad máxima de datos de 1.3 Gbps en la banda de 5 GHz y 600 Mbps en la banda de 2.4 GHz, los puntos de acceso de la serie 220 son tres veces más rápidos que los puntos de acceso 802.11n y ofrecen un rendimiento similar al de una conexión por cable.
  - Incluyen la tecnología ClientMatch, que elimina a los clientes adherentes mediante la recopilación continua de métricas de rendimiento de la sesión desde dispositivos móviles.
  - Tres antenas integradas omnidireccionales con inclinación hacia abajo (AP-224) y tres conectores de antena externos diplexados combinados (AP-225).
  - Precio elevado (1295 euros).

De los anteriores modelos todos cumplen las siguientes características:

- Máximo de 255 conexiones concurrentes.
- Alimentación directa de CC y alimentación a través de Ethernet (PoE).
- Número máximo de SSID es 16.

4.1.2.3 Puntos de acceso de exterior

Requisitos que deben satisfacer los puntos de acceso de exterior:

- Máximo de 255 conexiones concurrentes.
- Exposición a temperaturas extremadamente altas y bajas, humedad y precipitación persistentes.
- Diseño estético y poco llamativo.
- Velocidad de datos máxima de 1.3 Gbps en la banda de 5 GHz y 600 Mbps en la banda de 2.4 GHz.
- Alimentación a través de Ethernet (PoE).
- Número máximo de SSID es 16.
- Antena direccionales.

Existen dos modelos externos de **Cisco** cuyas principales diferencias respecto al resto son:

- Aironet 1532I
  - Dimensiones/peso 23 cm (ancho) x 10 cm (fondo) x 17 cm (alto) / 2,3kg
  - 3x3 MIMO con 3 transmisiones espaciales (2.4 GHz) y 2x3 MIMO con 2 transmisiones espaciales (5 GHz).

  - Antenas internas omnidireccionales.
  - Precio bajo (1490 euros).

- Aironet 1532E
  - Dimensiones/peso 26 cm (ancho) x 10 cm (fondo) x 17 cm (alto) / 2,3kg
  - MIMO 2x2 con 2 transmisiones espaciales (2.4 GHz) y MIMO 2x2 con 2 transmisiones espaciales (5 GHz).
  - Antenas externas omnidireccionales.
  - Precio bajo (1295 euros).

Existen cuatro modelos externos **Aruba HP** cuyas principales diferencias respecto al resto son:

- AP-274
  - Dimensiones/peso 23 cm (ancho) x 24 cm (fondo) x 19 cm (alto) / 2,4kg
  - Bandas de radio de 2,4 GHz (600 Mbps máx.) y 5 GHz (1,3 Gpbs máx.), cada una de ellas con MIMO 3x3 y tres conectores de antena externos.
  - Precio bajo (1195 euros).

- AP-275
  - Dimensiones/peso 23 cm (ancho) x 24 cm (fondo) x 27 cm (alto) / 2,4kg
  - Bandas de radio de 2,4 GHz (600 Mbps máx.) y 5 GHz (1,3 Gpbs máx.), cada una de ellas con MIMO 3x3 y tres antenas omnidireccionales integradas.
  - Precio medio (1695 euros).

- AP-277
  - Dimensiones/peso 23 cm (ancho) x 22 cm (fondo) x 13 cm (alto) / 2,1kg
  - Bandas de radio de 2,4 GHz y 5 GHz, cada una de ellas con MIMO 3x3 y tres antenas direccionales de ancho de haz de 80° H x 80° V integradas.
  - Precio alto (2005 euros).

- AP-365
  - Dimensiones/peso 165 mm (ancho) x 165 mm (largo) x 110 mm (alto) / 807 g
  - Bandas de radio de 2,4 GHz (400 Mbps máx.) y 5 GHz (867 Mpbs máx.), cada una de ellas con 2x2 MIMO y antenas omnidireccionales integradas.
  - Precio alto (1085 euros).

4.1.3 Elección y compra del equipamiento

La selección de los puntos de acceso se lleva a cabo en función de las necesidades de la sede, las prestaciones que ofrece cada uno de ellos y el presupuesto económico. La elección más adecuada reside en el modelo AP-207 como punto de acceso interior ya que supone un mayor ahorro y disminuye los problemas que puedan causar la integración de un punto de acceso Cisco en una Red Corporativa con tecnología Aruba.

Todos los puntos de acceso Aruba incorporan la tecnología Adaptive Radio Management (ARM), que optimiza el comportamiento Wi-Fi garantizando que los puntos de acceso se mantengan libres de interferencias por radiofrecuencias. También incluye la tecnología patentada ClientMatch, que recopila continuamente mediciones de rendimiento de la sesión de los dispositivos móviles y se utilizan para dirigir inteligentemente a los clientes hacia el mejor punto de acceso, con la señal Wi-Fi más fuerte. Esta es una característica que ofrecen todos los productos Aruba, al revés que su competidor Cisco, garantizan la igualdad de recursos para todos sus clientes siguiendo una campana de Gauss.

El radio de cobertura estimado para dicho punto de acceso está entre 20 y 25 metros. La alimentación de los equipos se realiza mediante PoE, estándar (IEEE 802.3af), permite la alimentación en corriente continua de equipos mediante el propio cable Ethernet. Para conseguir esta telealimentación se utiliza el switch con el que ya cuentan.

Dentro de las redes inalámbricas que ofrece Aruba existen dos tipos de depliegues inalámbricos. El primero, que suele utilizarse en sedes de grandes dimensiones, incorporan una controladora física local que gestiona el tráfico y controla los puntos de acceso. La segunda, que suelen utilizarse en sedes más pequeñas, crea un clúster de puntos de acceso donde uno de ellos actúa como controladora virtual gestionando todo el tráfico además de los propios puntos de acceso. Según el tamaño de este despliegue se va a elegir el modelo de sede Instant con controladora virtual.

La selección de los puntos de acceso de exterior se lleva a cabo entorno a las características como Client Match, ARM y al precio. Debido al elevado costo de los puntos de acceso exteriores, se decide seleccionar el AP-365, que incorpora 802.11ac Wave 2, radio dual, 5 GHz 802.11ac y 2.4 GHz 802.11n. Bien es cierto, que uno de los requisitos técnicos a implementar es poder contar con puntos de acceso que incorporen antenas direccionales. Esto lo cumple la serie 270 de puntos de acceso exteriores, pero el precio es muy elevado. Se considera que, relación calidad-prestaciones-precio, la mejor opción es la serie 360 más concretamente el modelo 365. A cambio de carecer de antenas direccionales se obtiene Wave 2, que utiliza tecnología MU-MIMO y otros avances para ayudar a aumentar las velocidades inalámbricas máximas teóricas de 3,47 Gbps.

(a) Punto de Acceso (b) Punto de Acceso back (c) Punto de acceso exterior (d) Punto de acceso exterior back

Figura 4.12 Puntos de acceso interiores y exteriores.

Conclusiones tras análisis y elección de los puntos de acceso

La elección recae en el modelo interior AP-207 y modelo exterior AP-365, ambos de **Aruba HP**.

4.2 Cableado Estructurado

4.2.1 Suministro del cableado para nuevos puntos de acceso

El cableado estructurado utilizado por los puntos de acceso tanto externos como internos es de nueva instalación lo que se resumen en doce nuevos canales. Por tanto es necesario el despliegue de doce nuevos enlaces permanentes de Cat6A, y veinticuatro nuevos latiguillos de Cat6A para poder conectar cada punto de acceso con la toma, así como para unir el switch y el panel de parcheo. A continuación se resumen las necesidades de cableado estructurado de cada planta de la sede.

- **Planta baja**

  Esta planta es la que mayor uso tiene del edificio principal, en ella se encuentra la oficina de los empleados de la sede y la recepción, ambas salas cuentan con tomas de red ya instaladas. Este hecho hace que el cableado de los puntos de acceso comparta la canalización del despliegue inicial y solo se necesite añadir los enlaces permanentes Cat6A y las tomas de red de Cat6A correspondientes. De igual forma ocurre con el punto de acceso que se sitúa en la parte porterior de esta planta baja, utiliza la canalización de las tomas que existe en esta sala. Respecto al punto de acceso exterior situado en la fachada del edificio principal es necesario una canalización externa.

  Como resultado se obtiene:

  - Incorporar 4 tomas de red a Cat6A.
  - Incorporar 4 enlaces permanentes de Cat6A desde la toma de red hasta el panel de parcheo por las canalizaciones existentes.
  - Incorporar 8 latiguillos de Cat6A.
  - Incorporar canalización externa.

- **Planta primera**

  Esta planta es utilizada para exposiciones y cócteles de día, en ella se encuentran dos salas que se alquilan para eventos de todo tipo además de una azotea. El despacho de dirección y la secretaría se sitúan en esta planta también y cuentan con un equipo fijo en cada una de las salas. Los tres puntos de acceso necesitan nuevos enlaces permanentes y tomas de red, ambas de Cat6A, que se despliegan desde el CPD hasta la localización de los mismos mediante el pasamuros del cableado vertical utilizando las canalizaciones del despliegue existente. El punto de acceso exterior necesita una nueva canalización externa.

  Como resultado se obtiene:

  - Incorporar 3 toma de red de Cat6A.
  - Incorporar 3 enlace permanente de Cat6A desde la toma de red hasta el panel de parcheo.
  - Incorporar 6 latiguillos de Cat6A.
  - Incorporar canalización externa.

- **Salón de actos, biblioteca y sala de exposiciones**

  Esta planta es la más utilizada por los visitantes del parque, en ella se encuentra el salón de actos, la biblioteca y una sala de estudio además de un patio interior y otro exterior. El salón de actos cuenta con dos equipos fijos por lo que el nuevo enlace permanente comparte esta canalización. En la biblioteca y la sala de exposición existen tomas sin uso aunque por petición del organismo se decide no reutilizarlas, por lo que en estas estancias el cableado, canalización y tomas de red son de nueva instalación. Los puntos de acceso exteriores necesitan una canalización exterior.

  Como resultado se obtiene:

  - Incorporar 5 tomas de red de Cat6A.
  - Incorporar 5 enlaces permanentes de Cat6A desde la toma de red hasta el panel de parcheo.
  - Incorporar 10 latiguillos de Cat6A.

– Incorporar 2 canalizaciones externas.

4.2.2 Sustitución del cableado necesario

Tras la certificación del cableado estructurado inicial se toma la decisión de sustituir:

- **Cableado estructurado de Cat6.**

  Tras la certificación del cableado se observa la necesidad de cambiar dos de los enlaces. El primer enlace pertenece al ordenador de mesa que está en la biblioteca del edificio anexo mientras que el segundo enlace pertenece a la impresora que se sitúa en la planta baja del edificio principal. Para este cableado se utilizará una bobina de Cat6A además de los conectores RJ45 macho necesarios.

- **Latiguillos de Cat5e.**

  Se deciden cambiar todos los latiguillos existentes de esta categoría ya que empeoran el rendimiento del canal. Se sustituyen por latiguillos BlueLine GigaLink de 4 pares RJ45-RJ45 de Cat6A UTP cuya longitud es de 1 metro cada uno. Soporta una transmisión de datos de hasta 10Gigabit Ethernet con un diámetro de 6 mm y color gris lo que facilita ocultarlo y camuflarlo en lugares visibles.

- **Tomas de red de Cat6.**

  Tras consenso con los responsables de la sede se decide sustuir las dos tomas de red que pertenecen a los enlaces permanentes que se sustituyen. Se incorporan dos nuevas tomas de red de Cat6A.

  Como resumen:

  – Sustitución de 24 latiguillos de Cat5e por Cat6A.

  – Sustitución de 2 enlaces permanentes de Cat6 a Cat6A por fallo en la certificación.

  – Sustitución de 2 tomas de red de Cat6 a Cat6A.

Conclusiones sobre el cableado estructurado

En la siguiente tabla podemos observar el sumario de elementos que se necesitan:

Nuevo equipamiento	
Elementos	Cantidad
Aruba AP-207 Dual 2x2:2 802.11ac AP	8
Aruba AP-275 outdoor Dual 3x3:3 802.11ac AP	4
Licencia "Aruba controller per AP Capacity"	12
Licencia "Aruba controller per AP PEF"	12
Licencia "Aruba controller per AP RF Protect"	12
Latiguillos Cat6A UTP RJ-45 para equipos finales, impresora y proyector	24
Latiguillos Cat6A UTP RJ-45 para puntos de acceso	24
Panel de parcheo 24 puertos UTP RJ-45 Cart6A	1
Tomas de red Cat6A	14
Enlaces Permanentes Cat6A para solucionar los problemas detectados	2
Enlaces Permanentes Cat6A para nuevos puntos de acceso	12
Canalizaciones	8

4.3 Diseño físico

El diseño físico de la red de la sede reutiliza el router y el switch de la arquitectura inicial de la sede además de los ocho equipos fijos, una impresora y un proyector (con sus respectivos latiguillos y enlaces permanentes) conectados tal y como se muestra en la siguiente tabla.

Tabla 4.1 Puertos del switch ocupados por la arquitectura inicial.

Puertos del switch ocupados por la arquitectura inicial			
Planta	Sala	Numero de puerto	Descripción
Baja	CPD	GE1/0/1	Router
Baja	Recepción	GE1/0/12	Equipo fijo
Baja	Oficina izquierda	GE1/0/6	Equipo fijo
Baja	Oficina izquierda	GE1/0/2	Equipo fijo
Baja	Oficina izquierda	GE1/0/4	Impresora
Baja	Oficina derecha	GE1/0/11	Equipo fijo
Baja	Oficina derecha	GE1/0/22	Equipo fijo
Anexo	Salón de actos	GE1/0/7	Equipo fijo
Anexo	Salón de actos	GE1/0/10	Proyector
Anexo	Biblioteca	GE1/0/8	Equipo fijo
Anexo	Sala de estudios	GE1/0/9	Equipo fijo

El nuevo diseño de red contará con doce puntos de acceso conectados al switch en los puertos que se encuentran libres tal y como muestra la siguiente tabla.

Tabla 4.2 Puertos del switch ocupados por los puntos de acceso.

Puertos del switch ocupados por los puntos de acceso				
Planta	Sala	Numero de puerto	Descripción	Tipo
Baja	Porche de arcos	GE1/0/3	AP-1	Exterior
Baja	Oficina izquierda	GE1/0/5	AP-2	Interior
Baja	Recepción	GE1/0/19	AP-3	Interior
Baja	Oficina fondo	GE1/0/13	AP-4	Interior
Primera	Oficina derecha	GE1/0/14	AP-5	Interior
Primera	Oficina izquierda	GE1/0/15	AP-6	Interior
Primera	Azotea	GE1/0/16	AP-7	Exterior
Anexo	Salón de actos	GE1/0/17	AP-8	Interior
Anexo	Biblioteca	GE1/0/18	AP-9	Interior
Anexo	Sala de estudios	GE1/0/20	AP-10	Interior
Anexo	Patio exterior	GE1/0/21	AP-11	Exterior
Anexo	Patio exterior	GE1/0/23	AP-12	Exterior

La integración de la sede con la Red Corporativa de la empresa se muestra en la topología de la Figura 4.13:

Figura 4.13 Integración en Red Corporativa.

4.4 Diseño lógico

Tal y como se nombra en capítulos anteriores, para este diseño se ha seleccionado el tipo de despliegue con controladora virtual (VC). Este tipo de arquitectura tiene la característica de que uno de los puntos de acceso actúa como controladora del resto. La VC se encarga de que la configuración esté sincronizada en todos los puntos de acceso del clúster.

4.4.1 Gestión de usuarios

El diseño lógico se realiza en torno a la gestión de usuarios, que son clasificados según la conmutación de su tráfico y los accesos con los que cuentan:

- **EMPLEADOS**

  Usuarios que se conectan al servicio WI-Fi, son empleados de la sede.

  - Conmutación del tráfico

    Nivel 2 en local en la VLAN designada para ello

  - Acceso

    A los recursos locales, los servicios horizontales y a Internet.

  - Direccionamiento

    Servidor DHCP local.

- Autenticación

  La autenticación y autorización del usuario se realizará mediante 802.1x contra el servidor RADIUS central.

- **ITINERANTES**

Usuarios que se conectan al servicio WI-Fi, son empleados de la empresa, pero no de la sede.

- Conmutación del tráfico

  Es tunelizado por un túnel GRE a nivel 2 desde el punto de acceso que actúa como controladora virtual hasta la controladora terminadora de túneles del nodo central donde es entregado a la VPN designada para ello.

- Acceso

  A los servicios horizontales y a Internet, y en ningún caso accederá a la red local del organismo desde el que se conecta.

- Direccionamiento

  Servidor DHCP centralizado. Para estos usuarios hay un pool de direcciones propias y comunes para toda la empresa.

- Autenticación

  La autenticación y autorización del usuario se realizará mediante 802.1x contra el servidor RADIUS central. Éste lo identifica como ITINERANTE tras asignarle una serie de parámetros que se definen en posteriores apartados.

- **INVITADOS**

Usuarios que se conectan al servicio WI-Fi, y son visitantes. Dicho acceso será de carácter temporal.

- Conmutación del tráfico

  Es tunelizado por un túnel GRE a nivel 2 desde el punto de acceso que actúa como controladora virtual hasta la controladora terminadora de túneles del nodo central, donde es entregado a la VPN designada para ello.

- Acceso

  A Internet, y en ningún caso accederá a la red local del organismo desde el que se conecta.

- Direccionamiento

  Servidor DHCP centralizado. Para estos usuarios hay un pool de direcciones propias y comunes para toda la empresa.

- Autenticación

  La autenticación del usuario se realizará mediante Portal Cautivo y la validación de ellos mediante envío de correo a una persona responsable, llamada sponsor.

4.4.1.1 VPN de la red

La Red Corporativa cuenta con tres VPN diferentes:

- **VPN INTERNET**

  Esta VPN es por la que salen a Internet los usuarios INVITADOS una vez que su tráfico ha sido tunelizado mediante el túnel GRE hasta la terminadora de túneles.

- **VPN ITINERANTE**

  Esta VPN es en la que conmuta el tráfico de los usuarios ITINERANTES una vez que su tráfico ha sido tunelizado mediante el túnel GRE hasta la terminadora de túneles.

- **VPN ENTRADA**

  Esta VPN es la que utilizan todas las sedes de la empresa para poder autenticarse contra el servidor RADIUS.

En la Figura 4.14 se representan los diferentes túneles que existen en la red. El túnel GRE está formado por el punto de acceso que actúa como controladora virtual hasta la terminadora de túneles del nodo central y se utiliza para enviar el tráfico que no debe conmutar en local, por él viajan el tráfico de los usuarios ITINERANTES e INVITADOS. Para la comunicación entre la controladora master y la terminadora de túneles también existe otro túnel GRE como medio para transmitir el tráfico de control ya que estas son controladas por la master.

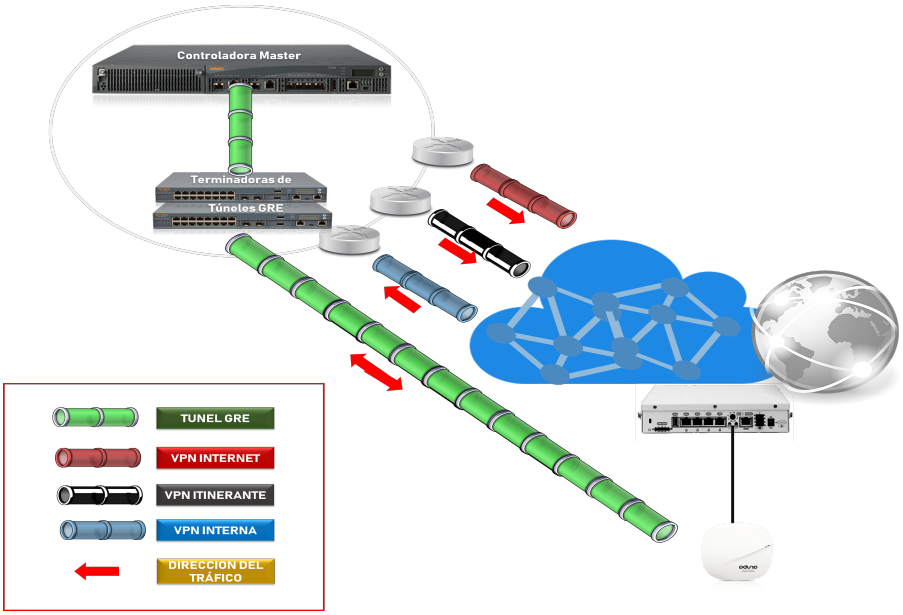


Figura 4.14 Túneles GRE y VPN.

4.4.2 SSIDs de la red

Encontramos dos tipos de SSIDs.

- **EMPLEADOS**

  Este SSID es compartido para los usuarios EMPLEADOS e ITINERANTES. El mecanismo de autenticación y autorización que utiliza es 802.1x contra el servidor RADIUS del nodo central que es el encargado de asignar dos roles diferentes, rol LOCAL o rol ITINERANTE. Estos son asignados según los parámetros de conexión de cada usuario y cada rol tiene asignada a una VLAN, un direccionamiento y unas políticas y restricciones propias. El rol LOCAL aporta la VLAN 20, el direccionamiento local de la sede y acceso completo (recursos locales, servicios horizontales e Internet) mientras que el rol ITINERANTE aporta la VLAN 4092, el direccionamiento centralizado del servidor DHCP del nodo central y acceso solo a servicios horizontales como el correo y a Internet.

- **INVITADOS**

  Este segundo SSID es utilizado por los usuarios INVITADOS. La autenticación del usuario se realizará mediante Portal Cautivo y para la autorización posterior se facilitan diferentes posibilidades a la sede, como son la validación de usuarios mediante envío de correo a una persona que pueda autorizar (sponsor), SMS, impresión de tickets... El rol INVITADOS aporta la VLAN 4093, direccionamiento centralizado del servidor DHCP del nodo central y acceso a Internet.

4.4.3 Clasificación de VLANs

El diseño lógico de la red inicial contaba con una única VLAN y un servidor DHCP con direcciones fijas en el rango privado 10.200.200.0/24. La arquitectura del nuevo diseño cuenta con separación lógica en VLANs, lo que proporciona mayor seguridad al aislar los diferentes tipos de tráfico y limitar los mensajes de difusión al segmento de red en el que se encuentre cada usuario. El servidor DHCP también es modificado, haciendo que asigne el direccionamiento según pertenezca a una VLAN u otra. En las siguientes tablas se observan las diferentes VLANs que existen en el nuevo diseño y los pools de direccionamiento.

Tabla 4.3 VLAN CONTROL.

VLAN CONTROL			
VLAN ID	DHCP	Pool IP	Esta VLAN se utiliza para la gestión de los puntos de acceso, su configuración y posterior seguimiento. Existe una dirección por punto de acceso y una fijada para la controladora virtual.
100	DHCP Local	10.200.200.0/26	

Tabla 4.4 VLAN FIJOS.

VLAN FIJOS			
VLAN ID	DHCP	Pool IP	Esta VLAN se utiliza para aportar direccionamiento a los equipos fijos, la impresora y el proyector.
10	DHCP Local	10.200.200.64/26	

Tabla 4.5 VLAN LOCAL.

VLAN LOCAL			
VLAN ID	DHCP	Pool IP	Esta VLAN se utiliza para los usuarios locales.
20	DHCP Local	10.200.200.128/25	

Tabla 4.6 VLAN ITINERANTE.

VLAN ITINERANTE			
VLAN ID	DHCP	Pool IP	Esta VLAN se utiliza para el trafico de los usuarios ITINERANTES.
4092	DHCP relay	10.10.10.0/22	

Tabla 4.7 VLAN INVITADOS.

VLAN INVITADOS			
VLAN ID	DHCP	Pool IP	Esta VLAN se utiliza para el trafico de los usuarios que pertenecen al servicio INVITADOS.
4093	DHCP relay	10.10.30.x/22	

En la Figura 4.15 se puede ver un esquema de cada una de las VLANs existentes en la sede.

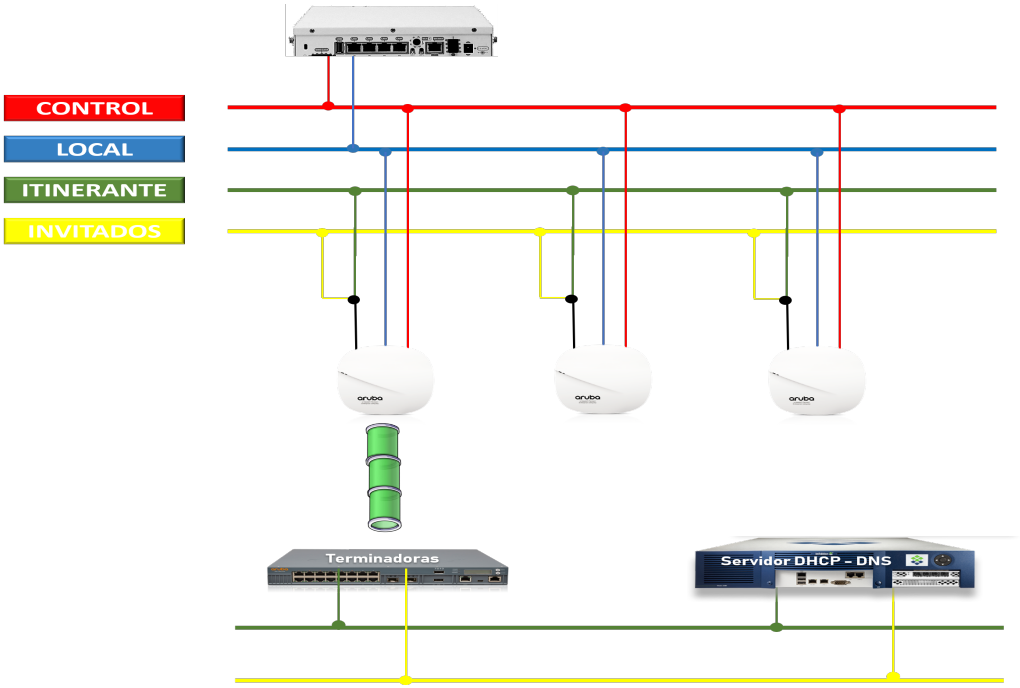


Figura 4.15 Representación de las diferentes VLANs.

4.4.4 Servicios de la red

El servidor DHCP centralizado autoriza y autentica mediante servicios definidos, cada uno de ellos cuenta con los siguientes componentes:

- **Categorización en el Servicio**

  Cuando una petición llega al servidor RADIUS recorre toda la lista de servicios y ejecuta aquel cuyas reglas de categorización cumpla. En esta pestaña es donde se definen los parámetros que debe tener una petición para que haga match contra este servicio.

- **Método de Autenticación**

  Cuando la petición ha hecho match en el servicio se le muestra los métodos de autenticación que utilizará para poder autenticarse. En esta pestaña se definen MSCHAPv2, EAP-PEAP.

- **Fuente de Autenticación**

  Tras conocer el método con el que se debe de autenticar, esta parte muestra contra qué fuente hacerlo. En esta pestaña es donde se define la conexión con su Active Directory.

- **Roles**

  Tras validar una solicitud contra la fuente de autenticación indicada, el servicio se encarga de asignar a cada cliente un rol según los parámetros con los que cuente ese usuario.

- **Aplicación de Políticas**

  En esta pestaña del servicio la petición ya cuenta con parámetros identificativos (como el ID de la sede, el punto de acceso desde el que se conecta, el SSID que son asignados durante la conexión) y con un rol (que puede ser LOCAL, ITINERANTE o INVITADO.). Con esta información se categoriza la petición y se le aplica un perfil donde se le asignan los permisos, las políticas y propiedades en la

navegación. Una vez que un usuario o máquina es autenticado se cambia la configuración del puerto al que están conectados a causa de la aplicación de una determinada política.

Este diseño requiere de dos servicios (EMPLEADOS e INVITADOS), cada uno de los cuales con unas políticas y unas restricciones propias.

- Servicio EMPLEADOS
  - Categorización del servicio:
    1. Verificar que el SSID del que proviene es EMPLEADOS.
    2. Verificar que la petición de autenticación proviene de un puerto inalámbrico.
    3. Verificar que el tipo de servicio es de autenticación.
  - Autenticación 802.1X:
    1. El método de autenticación debe ser MSCHAPv2 como principal.
    2. La fuente de autentización será tanto el Ative Directory de la empresa como la BBDD local del servidor de autenticación central.
  - Autorización:
    1. Los atributos utilizados para poder asignar roles posteriormente son obtenidos de las fuentes de autenticación anteriormente mencionadas, así como del contenido de la propia petición de autenticación.
  - Roles:
    1. El usuario que pertenece al grupo Sede-central del ActiveDirectory y pertenezca al grupo de puntos de acceso llamado Sede20, se le asigna el rol LOCAL.
    2. El usuario que no cumple la condición anterior, se le asigna el rol ITINERANTE.
  - Aplicación de políticas:
    1. Las políticas asignadas al rol LOCAL es acceso a los servicios horizontales, servicios locales e Internet.
    2. Las políticas asignadas al rol ITINERANTE es acceso a los servicios horizontales e Internet.

- Servicio INVITADOS:
  - Categorización del servicio:
    1. Verificar que el SSID del que proviene es INVITADOS.
    2. Verificar que la petición de autenticación proviene de un puerto inalámbrico.
    3. Verificar que la MAC del usuario no sea su nombre de usuario.
  - Autenticación 802.1X:
    1. El método de autenticación debe ser PAP como principal.
    2. La fuente de autentización será la BBDD de usuarios invitados, que es local del servidor de autenticación central.

- Autorización:
  1. Los atributos utilizados para poder asignar roles posteriormente son obtenidos de las fuentes de autenticación anteriormente mencionadas, la BBDD local de tiempo, la BBDD local de dispositivos, así como del contenido de la propia petición de autenticación.

- Roles:
  1. El usuario que se ha registrado desde el portal y lo haya validado un sponsor, se le asigna el rol INVITADOS.

- Aplicación de políticas:
  1. Las políticas asignadas al rol INVITADOS es acceso a Internet.
  2. Las políticas asignadas al rol ITINERANTE es acceso a los servicios horizontales e Internet.

4.4.5 Seguridad de la red

Métodos de autenticación:

- Autenticación por 802.1x (usuario y máquina). [EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC]
- Autenticación MAC (máquina).
- Autenticación Web basado en portal cautivo (usuario).

Fuentes de autenticación

- Base de datos interna del servidor de autenticación centralizado, donde se almacenan los usuarios INVITADOS.
- Active Directory de la empresa donde se encuentran registrados todos los empleados y personal laboral de la misma.

5 Configuración y despliegue de la red

"No hay mal que por bien no venga"

JOSÉ RAÚL CANO GARCÍA

5.1 Configuración switch y router

La configuración del equipo de nivel 2 (switch) se basa en incorporar las nuevas VLANs que han sido diseñadas y asignarlas a los puertos correspondientes. Los doce puertos donde se colocan los puntos de acceso son PoE y son configurados como trunk 802.1q para la VLAN 100 (CONTROL) como nativa (untagged) y para el resto de VLANs como tagged.

La configuración del equipo de nivel 3 (router) radica en definir todas las interfaces e incorporar las direcciones IP para la VLAN 100, VLAN 10 y VLAN 20.

A continuación se observa la configuración que es añadida al switch y al router de la sede.

Configuración equipo de nivel 2

```
ip default-gateway 10.200.200.1

vlan 10
name "FIJOS"
tagged 1,2,4,6-12,22
no ip address
exit

vlan 20
name "LOCAL"
tagged 1,3,5,13-21,23
no ip address
exit

vlan 100
name "CONTROL"
untagged 1,3,5,13-21,23
ip address 10.200.200.2 255.255.255.192
```

```
qos priority 1 management-vlan exit

vlan 4092
name "ITINERANTE"
 tagged 1,3,5,13-21,23
no ip address
exit

vlan 4093
name "INVITADOS"
 tagged 1,3,5,13-21,23,Trk1
no ip address
exit
```

Configuración equipo de nivel 3

```
dhcp enable

dhcp relay server-group 1 ip IP SERVIDOR DHCP LOCAL

dhcp relay server-group 1 ip IP SERVIDOR DHCP CENTRAL


interface Vlan-interface10
ip address 10.200.200.65 255.255.255.192
dhcp select relay
dhcp relay server-select 1

interface Vlan-interface20
ip address 10.200.200.129 255.255.255.128
dhcp select relay
dhcp relay server-select 1

interface Vlan-interface100
ip address 10.200.200.1 255.255.255.192
dhcp select relay
dhcp relay server-select 1
```

5.2 Configuración puntos de acceso

El punto de acceso puede configurarse de varias formas, aunque en este caso se opta por la carga de una plantilla lanzada desde el sistema de monitorización central hasta el punto de acceso que actúa como controladora virtual. Los pasos a seguir son:

1. Conectar el punto de acceso mediante un cable ethernet al puerto POE del switch.
2. Asignar dirección IP al punto de acceso mediante el servidor DHCP local.
3. Localizar sistema de monitorización central, estos son los pasos:

- El punto de acceso localiza la dirección del sistema de monitorización central mediante la opción 60 y la opción 43 definida en el servidor DHCP local.
- El punto de acceso inicia la petición DHCP con la opción 60 "ArubaInstantAP". En el servidor de DHCP se procesa esta petición, y tras verificar la existencia de la opción 60, ratifica que tiene configurada la opción 43, para poder responderle con la IP del sistema de monitorización central.
- Una vez que el punto de acceso localiza al sistema de monitorización central, se asocia al grupo Sede20.
- Este grupo contiene la plantilla de configuración, lo que provoca que todos los puntos de acceso de este grupo tengan la misma configuración.
- Una vez que la plantilla está creada y definida, se vuelca sobre el punto de acceso que actúa como controladora virtual y de aquí se extiende al resto de puntos de acceso del clúster.

Los parámetros de la plantilla son los siguientes:

Tabla 5.1 Parámetros plantilla de configuración 1.

Plantilla configuración	
Parámetro	Significado
version 6.5.1.0-4.3.1	Asigna un número de versión para el IAP.
virtual-controller-country ES	Especifica el país de operación.
virtual-controller-ip ipaddressvc	Asigna una dirección IP para el controlador virtual.
terminal-access	Permite el acceso a la CLI del punto de acceso virtual.
ntp-server Ipservidor	Configura la dirección IP o la URL (nombre de dominio) del servidor NTP.
clock summer-time	Configura el horario de verano.
dynamic-radius-proxy	Habilita la función de proxy para permitir que los AP del clúster use la dirección IP del Controlador Virtual cuando se comunica con los servidores RADIUS.
allow-new-aps	Permite nuevos puntos de acceso en el dominio.
routing-profile	Crea un perfil de enrutamiento para enrutar el tráfico al túnel VPN.
snmp-server conmmunity	Este comando configura los parámetros SNMP.
arm	Asigna un perfil de Adaptive Radio Management (ARM) para IAP y configura las funciones de ARM.
wide-bands 5ghz	Asigna banda de 5GHz.
80mhz-support	Permite el uso de canales de 80 MHz en AP con radios de 5 GHz.
min-tx-power 15 max-tx-power 18	Establece la potencia de transmisión máxima y mínima.
band-steering-mode prefer-5ghz	Permitir que el IAP dirija al cliente a la banda de 5 GHz (si el cliente tiene capacidad de 5 GHz).
air-time-fairness-mode fair-access	para asignar espacio de tiempo uniformemente a todos los clientes.
scanning	Permite a los IAP escanear otros canales.
syslog-level	configura los niveles de instalación de syslog.
extended-ssid	Permite configurar SSID adicionales.
vpn primary ip-address-controladora-master	Configura un servidor primario de Redes Privadas Virtuales (VPN) para conexiones VPN.

Tabla 5.2 Parámetros plantilla de configuración 2.

vpn backup ip-address-termiandora-tuneles	Configura un servidor VPN secundario o de respaldo para conexiones VPN.
vpn gre-outside	Habilitar la configuración automática del túnel GRE entre el controlador de Aruba para proporcionar conectividad L2.
mgmt-user admin contraseña	Configura las credenciales del usuario para acceder a la interfaz de usuario de administración del controlador virtual.
wlan access-rule <nombre>	Configura reglas de acceso para WLAN SSID o perfil cableado.
wlan ssid-profile EMPLEADOS	Configura un perfil WLAN SSID.
essid EMPLEADOS	Define un nombre que identifica de manera única una red inalámbrica.
captive-portal external	Configura la autenticación del portal cautivo.
mac-authentication	Habilita la autenticación MAC para los clientes que usan este perfil SSID.
g-min-tx-rate 6	Configura la especificación de la velocidad de transmisión mínima para la banda de 2,4 GHz.
a-min-tx-rate 9	Configura la especificación de la velocidad de transmisión mínima para la banda de 5 GHz.
mgmt-auth-server Clearpass	Configura los servidores de autenticación para la interfaz de usuario de administración del controlador virtual.
wlan auth-server Clearpass	Configura un servidor RADIUS y CPPM externo para la autenticación del usuario.
wlan external-captive-portal	Configura los perfiles para el portal cautivo externo.
ip dhcp ITINERANTE/INVITADO	configura los modos y ámbitos de asignación de DHCP para la red.
server-type Centralized,L2	Define el modo de direccionamiento distribuido a nivel 2.
server-vlan 4092/4093	Configura una ID de VLAN para el alcance de DHCP.
wired-port-profile nombre	configura un perfil de puerto cableado para clientes IAP con cable.
opmode wpa2-aes	Configura la autenticación y el cifrado de capa 2 para este SSID.WPA2 con encriptación AES y claves dinámicas usando 802.1x.
vlan 4092	Permite a los administradores asignar una VLAN a los usuarios de SSID.
auth-server Clearpass	Configura un servidor de autenticación para los usuarios de SSID.
set-vlan Aruba-User-Role equals LOCAL 1	Asigna una VLAN a los clientes que son de tipo rol LOCAL.
enforce-dhcp	Aplica la asignación dinámica de VLAN para clientes desde el servidor DHCP.

En el anexo se encuentra la plantilla de configuración que se ha realizado para la configuración de la sede.

5.3 Configuración del servidor de autenticación

El servidor RADIUS central es el que autentica, autoriza, aplica roles y políticas mediante un servicio según las características de cada petición del usuario. Los diferentes parámetros que se le asignan a una petición de autenticación tras pasar por un servicio son:

- Rol (Aruba-User-Role) puede ser EMPLEADO, ITINERANTE e INVITADOS.
- VLAN (Aruba-named-VLAN) puede ser LOCAL, ITINERANTE o INVITADO
- Políticas, que otorgan accesos y restricciones a la red de forma total o parcial.

Los procedimiento y pasos genéricos para crea un servicio son:

1. **Configuración del servicio**
    - La pestaña Service (Servicio) proporciona los parámetros básicos de configuración.
    - La pestaña Service rule (Reglas del servicio) define un conjunto de criterios y reglas que las peticiones de autenticación deben cumplir para poder hacer match contra el servicio.

Tabla 5.3 Parámetros de configuración del servicio.

Parámetro	Descripción
Tipo	Seleccionar el tipo de servicio que se utiliza (802.1x Wireless, MAC Authentication, RADIUS Enforcement)
Nombre	Nombre del servicio
Descripción	Información adicional que ayuda a identificar el servicio
Mas opciones	Marcar la pestaña autorización para poder acceder a sus pestañas de configuración.

Tabla 5.4 Parámetros para crear una regla.

Parámetro	Descripción
Tipo	Seleccionar tipo de regla de servicio (RADIUS Cisco, RADIUS Aruba, RADIUS IETF, Authentication)
Nombre	Nombre de la regla de servicio existente en la lista desplegable
Operador	Seleccionar un operador entre BELONGS-TO, NOT-BELONGS-TO, CONTAINS o EQUALS
Valor	Seleccionar el valor de la lista desplegable o introducir manualmente.

2. **Configuración de Autenticación**
    - La pestaña Autenticación contiene opciones para configurar métodos de autenticación y fuentes de autenticación.
3. **Configuración de Autorización**
    - La pestaña Autorización se usa para seleccionar las fuentes de autorización para este servicio. El servidor de autenticación central es capaz de recuperar atributos asignados a cada petición de autenticación. Esta información la extrae de las fuentes de autorización, independientemente de qué fuente de autenticación se utilizó para autenticar al usuario. Para un servicio determinado, los atributos se obtienen de fuentes de autorización tales como el "Endpoint Repository".

Tabla 5.5 Parámetros de autenticación.

Parámetro	Descripción
Métodos de autenticación	Seleccionar métodos de autenticación utilizando el campo “Seleccionar para agregar” (Select to Add) utilizado para este servicio. (EAP PEAP, EAP TLS, EAP TTLS, EAP MSCHAPV2)
Fuentes de autenticación	Especificar las fuentes de autenticación usando el campo “Seleccionar para Agregar” (Select to Add) , pueden ser locales ("Endpoints Repository", "Local User Repository") o remotas(Active directory)

4. Configuración de Roles

- La pestaña Roles es usada para asociar una política de asignación de roles (“Role Mapping Policy”) con este servicio. Esta se crea en "Add new Role Mapping Policy" añadiendo las condiciones y roles requeridos.

Tabla 5.6 Detalles de la política de asignación de roles.

Parámetro	Descripción
Descripción	Proporcionar información adicional sobre la política de asignación de roles seleccionada (“Rol Mapping Polity”)
Rol por defecto	Especificar el rol que se asignará cuando la petición no cumple ninguna de las condiciones
Algoritmo de evaluación de reglas	Seleccionar como deben valorarse las condiciones (probar todas o si machea contra la primera parar)

5. Configuración de Enforcement

- La pestaña Enforcement es usada para asociar una política de cumplimiento (“Enforcement Policy”) con este servicio. Ésta se crea en "Add new Enforcement Policy" añadiendo las condiciones y accesos o denegaciones requeridas.

Tabla 5.7 Parámetros de la configuración del Enforcement.

Parámetro	Descripción
Descripción	Muestrar información adicional sobre la política de cumplimiento seleccionada
Perfil por defecto	Especificar el acceso o degación que se asignará cuando la petición no cumple ninguna de las condiciones
Algoritmo de evaluación de reglas	Seleccionar como deben valorarse las condiciones (probar todas o si machea contra la primera parar)

5.3.1 Configuración servicio de autenticación con 802.1x

La autenticación 802.1x es la que utiliza el SSID EMPLEADOS, consta de tres componentes y se establece de la siguiente forma:

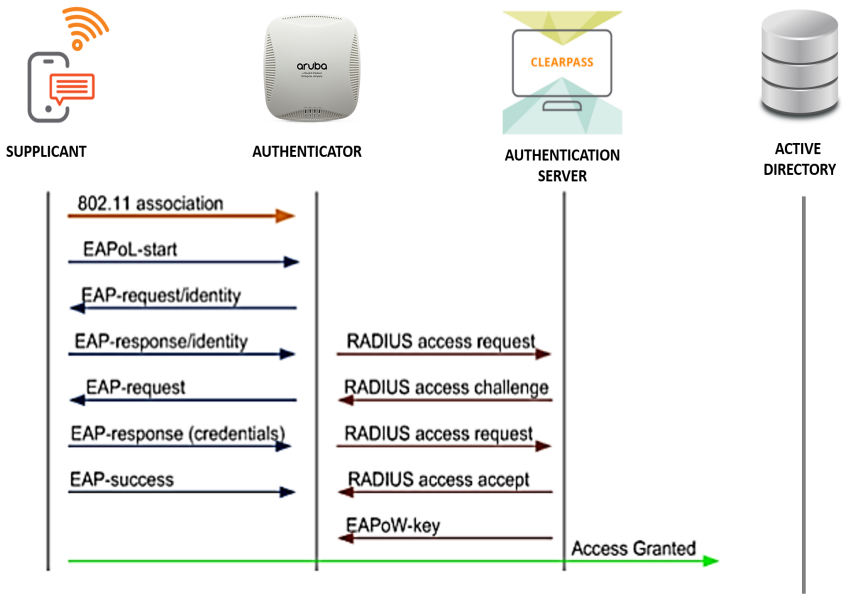


Figura 5.1 Descripción de autenticación de 802.11x.

1. RADIUS AccessRequest

   El punto de acceso que actúa como controladora (es el servidor de acceso a la red (NAS)) envía una solicitud de acceso RADIUS al servidor central, que luego evalúa e identifica los atributos de control.

2. Categorización del servicio

   En función de los atributos de control de conexión RADIUS identificados, la solicitud se categorizará en un servicio u otro.

3. Aplicación del servicio

   El servicio intenta autenticar al usuario utilizando el método de autenticación definido y lo autentica contra la fuente de autenticación o active directory de la empresa. Tras la respuesta correcta se procede a la asignación de roles que son establecidos por machear contra unas condiciones establecidas. Un rol significa una política asociada que es una forma de organizar a los usuarios y definir las restricciones y el tipo de acceso a la red.

4. RADIUS AccessAccept

   El servidor RADIUS responde al punto de acceso con un rol establecido y una VLAN prefijada. Este es capaz de interpretar estos parámetros definidos en la plantilla de configuración y lo mete en la VLAN correcta.

5. Petición DHCP

   Una vez que el usuario se encuentra en la VLAN correcta se produce la petición de dirección IP que será asignada por el servidor DHCP local en el caso de estar en la VLAN 20 (LOCAL) y el servidor central de direccionamiento en el caso de estar en la VLAN 4092 y 4093.

A continuación se observan todas las pestañas que componen el servicio EMPLEADOS del servidor de autenticación centralizado.

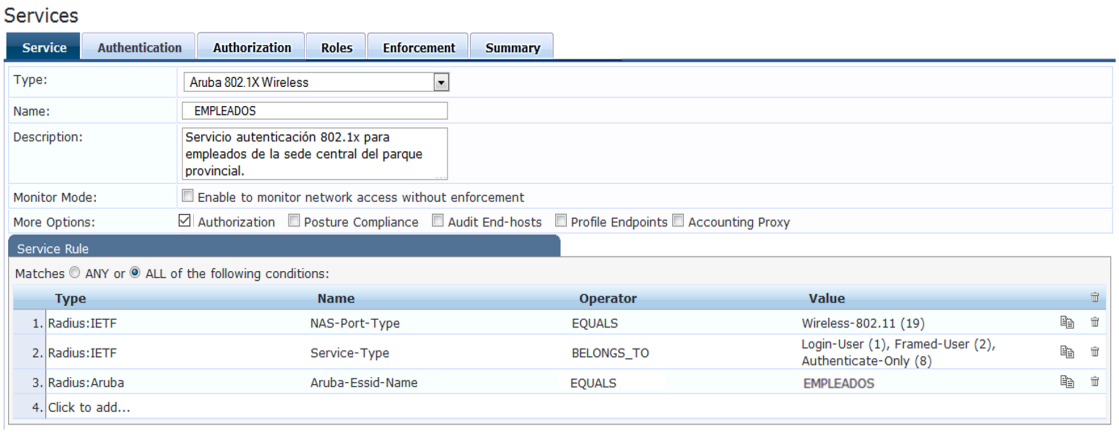


Figura 5.2 Configuración pestaña del servicio.

Radius:IETF > NAS-Port-Type > EQUALS > Wireless-802.11(19) Indica el tipo de puerto físico del NAS que está autenticando al usuario, según la norma RFC 2865 para categorizarlo como Wi-Fi.
Radius:IETF > Service-Type > BELONG-TO > (1),(2),(8) Indica el tipo de servicio que se proporciona. Login-User (1) = El usuario debe estar conectado a un host. Framed-User (2) = Utiliza protocolo PPP. Authenticate-Only (8) = Únicamente se devuelve al NAD la información de autenticación, no la de autorización.
Radius:Aruba > Aruba-Essid-Name > EQUALS > EMPLEADOS Indica que la petición debe venir desde el SSID EMPLEADOS.

Figura 5.3 Configuración pestaña de autenticación.

Active Directory Sistema de autenticación donde se encuentran ordenados por grupos los empleados de toda la empresa.
Local SQL DB Sistema de autenticación del servidor RADIUS donde se encuentran usuarios de gestión.

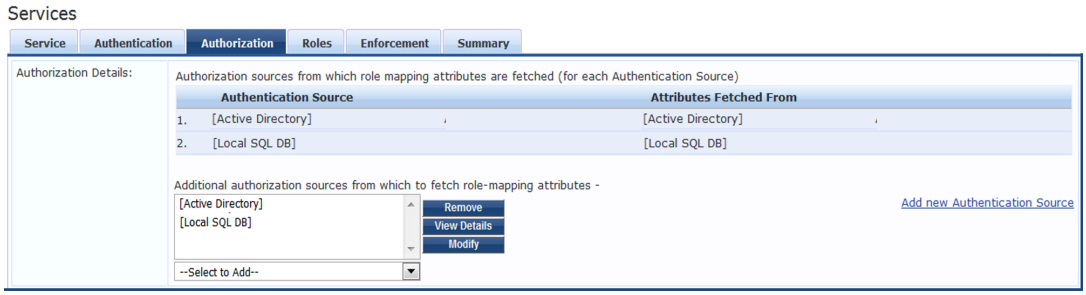


Figura 5.4 Configuración pestaña de autorización.

En la pestaña de autorización se nombran las fuentes de autenticacion seleccionadas en la pestaña anterior debido a que de éstas se seleccionaran los atributos necesarios para poder asignar roles, políticas y VLANs.

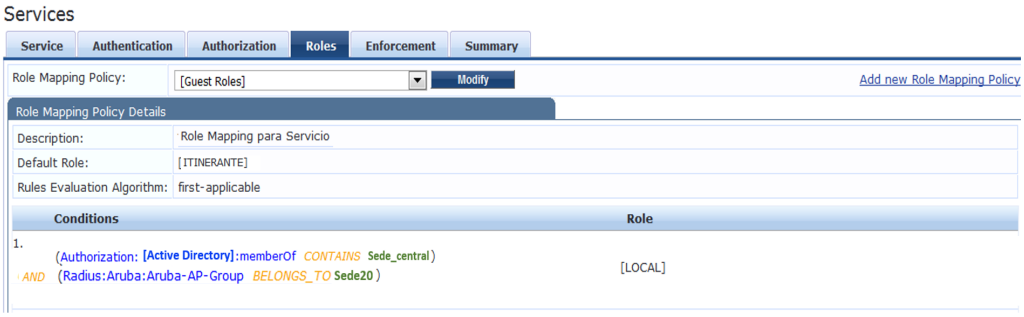


Figura 5.5 Configuración pestaña de roles.

Authorización: [Active Directory]:memberOf CONTAINS Sede-central El atributo "memberOf" obtenido del Ative Directory debe contener Sede-central.
Radius:Aruba:Aruba-AP-Group BELONGS-TO Sede20 El atributo "Aruba-AP-Group" obtenido desde la petición de autenticación debe ser Sede20

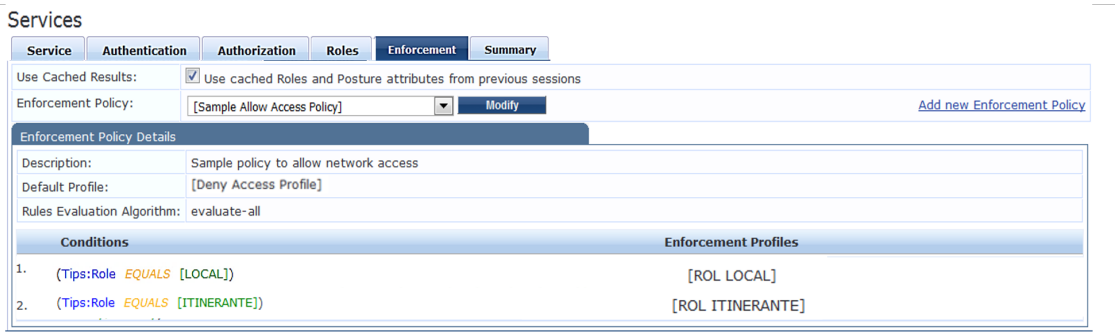


Figura 5.6 Configuración pestaña de enforcement.

Tips:Role EQUALS [LOCAL]
El atributo Tips recoge el rol que se le asigna en la pantalla anterior, éste debe ser igual a [LOCAL] para asignarle las políticas locales.
Tips:Role EQUALS [ITINERANTE]
El atributo Tips recoge el rol que se le asigna en la pantalla anterior, éste debe ser igual a [ITINERANTE] para asignarle las políticas de itinerancia.

5.3.2 Configuración servicio de autenticación con portal cautivo

La autenticación por portal cautivo se realiza a través de una redirección hacia dicha página tras la conexión del usuario a la red, así antes de poder tener acceso libre a Internet los usuarios de la red deben registrar los datos que se solicitan en el formulario del portal. El proceso de autenticación se muestra a continuación:

1. El usuario invitado asocia su dispositivo Wi-Fi al SSID INVITADOS y es redirigido hasta el portal cautivo y se le asigna el rol inicial de invitados (INVITADOS-ini) que tiene todo tipo de acceso restringido.
2. El portal cautivo cuenta con un formulario de inscripción que debe rellenar para poder acceder a la red donde los campos requeridos son:
   - Nombre
   - Correo
   - Correo del Sponsor o persona que autoriza el acceso y pertenece al personal de la sede.

   Una vez lo ha completado y enviado, el dispositivo del usuario vuelve a intentar la conexión. En este momento se produce la autenticación del usuario que será correcta si el sponsor ha validado su solicitud, es entonces cuando el servicio le asigna el rol final de invitados (INVITADOS).
3. Si por otro lado ya se ha registrado con anterioridad y cuenta con credenciales válidas y no expiradas puede acceder directamente.

Figura 5.7 Descripción de autenticación de usuarios invitados.

A continuación se observan todas las pestañas que componen el servicio INVITADOS del servidor de autenticación centralizado.

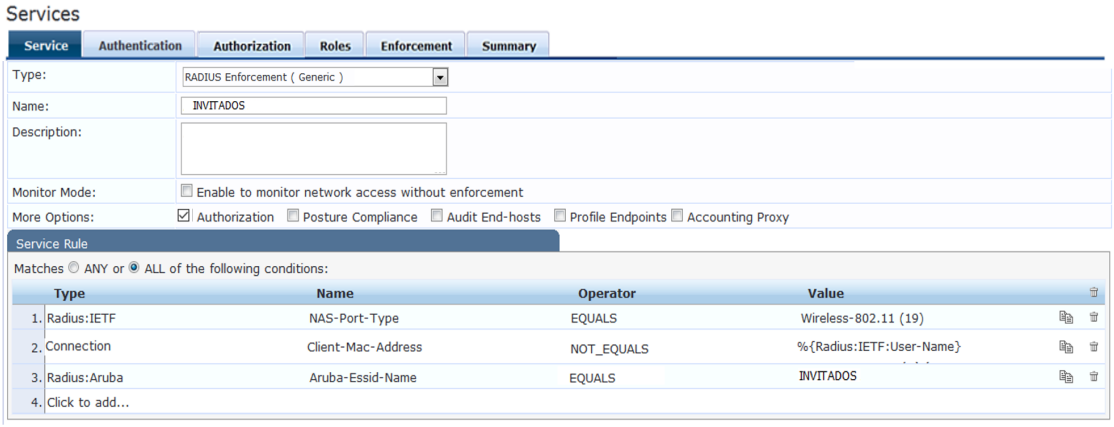


Figura 5.8 Configuración pestaña del servicio.

Radius:IETF > NAS-Port-Type > EQUALS > Wireless-802.11(19) Indica el tipo de puerto físico del NAS que está autenticando al usuario, según la norma RFC 2865 para categorizarlo como Wi-Fi.
Connection > Client-Mac-Address > NOT-EQUALS > Radius:IETF:User-Name Indica a que la autenticación debe tener como parémetro User-Name un argumento diferente a su MAC.
Radius:Aruba > Aruba-Essid-Name > EQUALS > INVITADOS Indica que la petición debe venir desde el SSID INVITADOS.

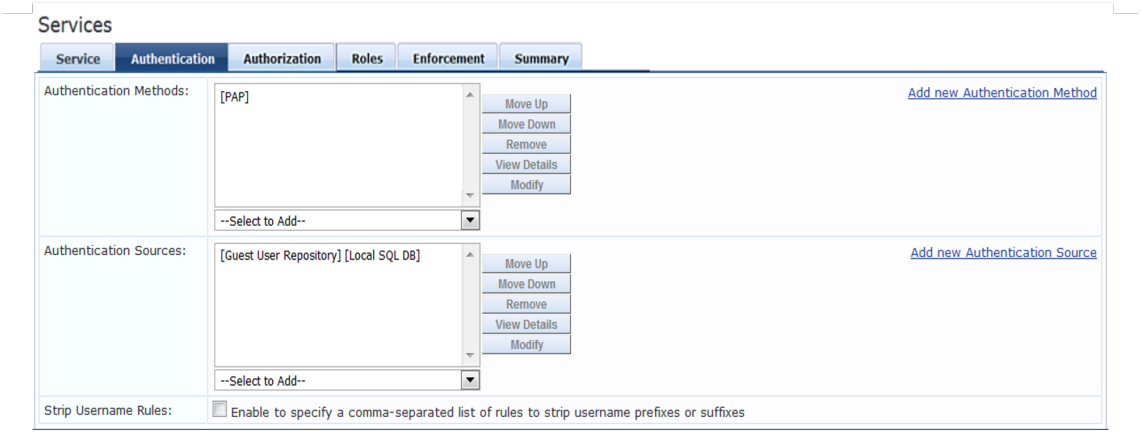


Figura 5.9 Configuración pestaña de autenticación.

Active Directory Sistema de autenticación donde se encuentran ordenados por grupos los empleados de toda la empresa.
Local SQL DB Sistema de autenticación del servidor RADIUS donde se encuentran usuarios de gestión.

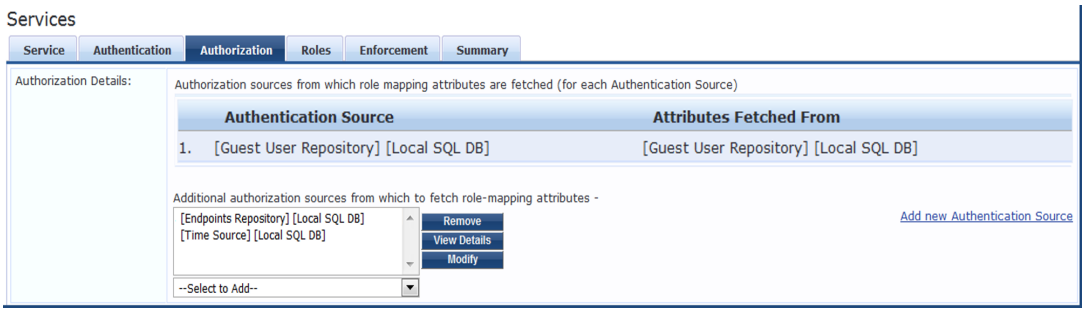


Figura 5.10 Configuración pestaña de autorización.

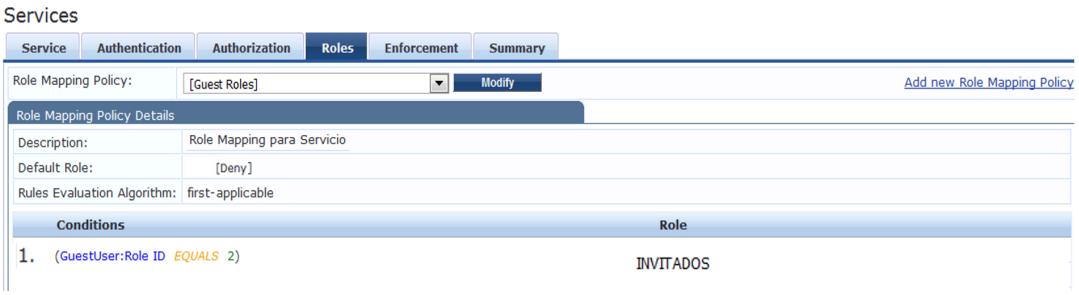


Figura 5.11 Configuración pestaña de roles.

GuestUser:Role ID EQUALS 2
El atributo "Role ID" obtenido de la base de datos interna GuestUser debe ser 2, lo que significa que se ha autenticado en el portal.

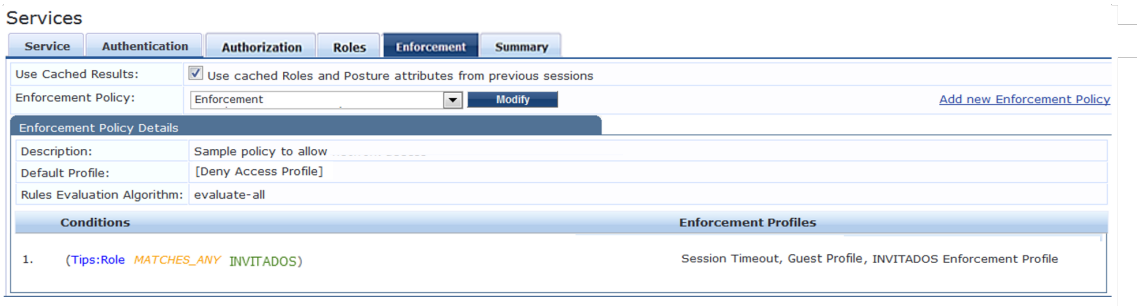


Figura 5.12 Configuración pestaña de enforcement.

Tips:Role EQUALS INVTADOS
El atributo Tips recoge el rol que se le asigna en la pantalla anterior, éste debe ser igual a INVITADOS para asignarle las políticas de invitados.

5.4 Configuración portal cautivo

La configuración del portal cautivo se rige por la creación del formulario inicial, de la página de inicio (útil cuando ya cuentas con credenciales) y las demás pantallas con mensajes informativos. En la sección de Autorregistros podemos ver la siguiente figura donde se configura uno a uno cada componente. El diagrama muestra el proceso de auto registro. Las flechas de color naranja sólido muestran el flujo de trabajo para el invitado y las de color azul muestran el flujo de trabajo para el administrador.

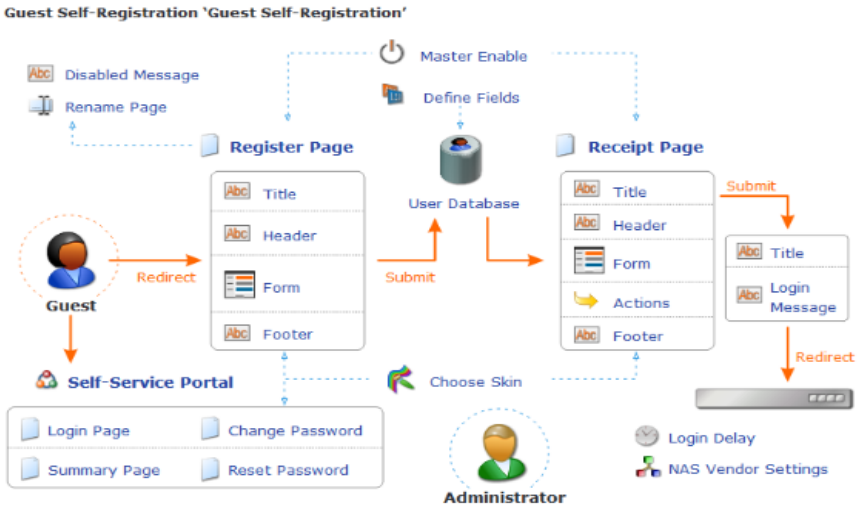


Figura 5.13 Configuración del Portal Cautivo.

.

- La Figura 5.14 se observa el formulario de registro que se encuentra en el portal cautivo.
- La Figura 5.15 se muestra relleno justo antes del momento de enviarlo.
- La Figura 5.16 se muestra el mensaje que aparece tras registrarse y enviar el formulario, aparecerá hasta que el sponsor valide la cuenta.

Figura 5.14 Página de registro del Portal Cautivo.

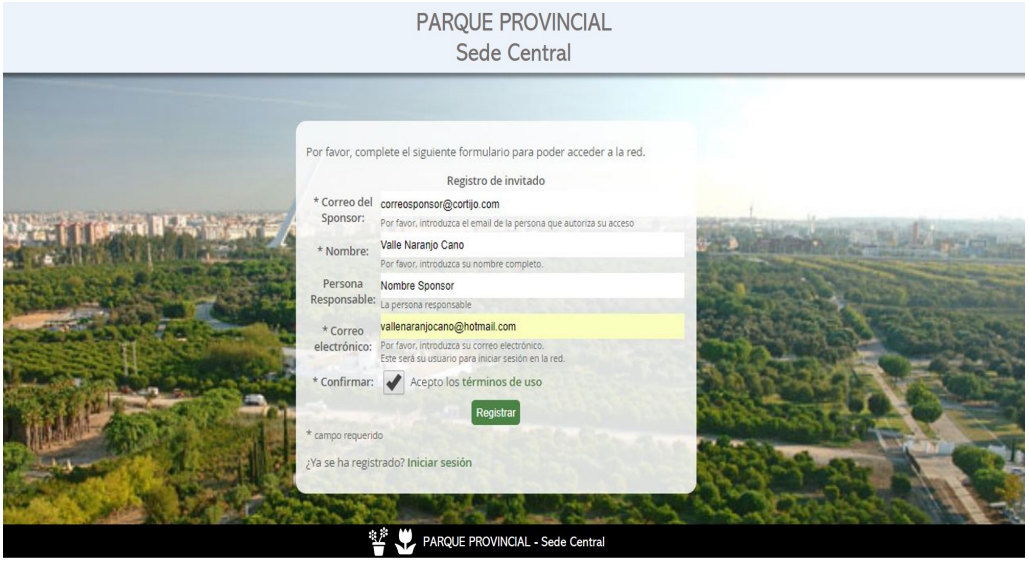


Figura 5.15 Formulario completo del Portal Cautivo.

.

Figura 5.16 Mensaje mostrado al usuario tras enviar el formulario..

Por otro lado al sponsor le llegará un correo donde podrá acceder a la siguiente pantalla y validar al usuario que le pide acceso. Tras la autorización el usuario invitado está validado y tiene acceso a internet durante un periodo de 24 horas.

- La Figura 5.17 muestra la pantalla que permite al sponsor validar la cuenta del usuario.
- La Figura 5.18 muestra el mensaje que le llega al usuario y tras él podrá acceder a la red.

Figura 5.17 Mensaje que le aparece al sponsor para validar a un usuario.

.

Figura 5.18 Mensaje que le aparece al usuario tras la validación del sponsor.

Para el desarrollo del portal cautivo se ha hecho uso de las siguientes tecnologías:

- HTML para la estructura del sitio web.
- JavaScript para la obtención de datos de usuario.
- PHP para el acceso y actualización de la base de datos, y validación de datos.

5.5 Configuración sistema de gestión de usuarios INVITADOS

Uno de los aspectos que se recogen en la toma de requisitos es la necesidad de una interfaz desde donde se puedan gestionar y controlar las cuentas de los usuarios INVITADOS. El sistema de autentización centralizado permite restringir las visibilidades y permisos de un usuario de administración para poder satisfacer esta necesidad. Este usuario con permisos especiales se denomina "Usuario Recepcionista".

La interfaz de gestión es un menú lateral donde se encuentran todas las opciones que puede realizar sobre las cuentas de usuarios tal y como se observa en la Figura 5.19.

Figura 5.19 Interfaz de gestión usuarios INVITADOS.

.

- **Crear cuentas**

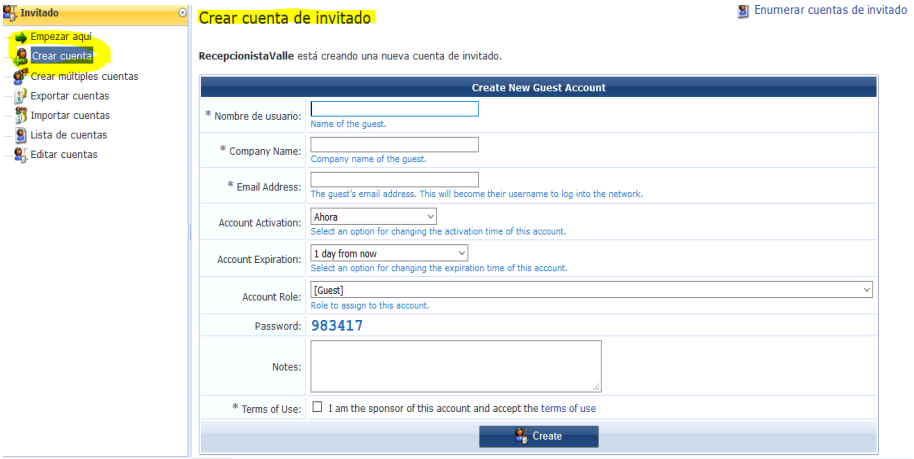


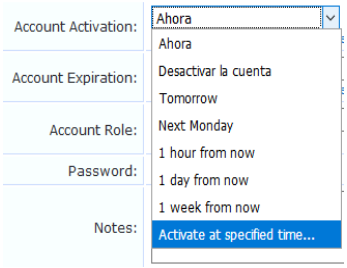
Figura 5.20 Interfaz de gestión usuarios INVITADOS - Crear cuenta.

.

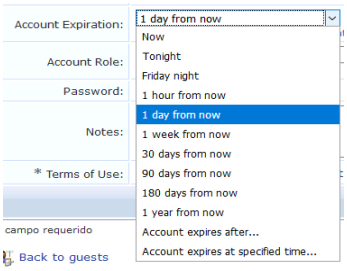
En esta pestaña se puede crear la cuenta o cuentas que se necesiten, pudiendo personalizar los siguientes parámetros:

- Nombre de usuario.
- Compañía del usuario.
- Dirección de correo electrónico.

– Instante de activación de la cuenta.



– Tiempo en el que expirará la cuenta.



El resultado es el siguiente:

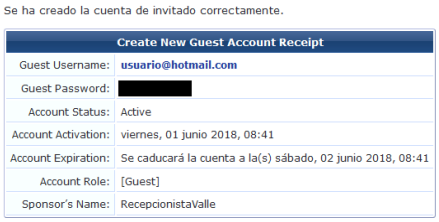


Figura 5.21 Nueva cuenta de usuario.

.

- **Crear múltiples cuentas**

  El procedimiento de creación de cuentas múltiples es el mismo que el de creación de una sola cuenta de usuario, simplemente se debe indicar el número de cuentas que se quieren crear.

- **Importar cuentas**

  Otra de las opciones disponibles es la exportación de cuentas de usuario definidas en un fichero tal y como muestran la Figura 5.22 y la Figura 5.23.

- **Listar cuentas**

  Con esta opción se puede ver todas las cuentas que se han creado, además pulsando sobre "Mostrar detalles" se observa toda la información que tiene el usuario tal y como muestra la Figura 5.24.

- **Editar cuentas**

  Con esta opción se pueden editar las cuentas de usuario que se hayan creado, se realiza seleccionando el usuario y pulsando sobre “Editar”. Aquí se podrá cambiar la contraseña de usuario y el tiempo de expiración de la cuenta tal y como muestra la Figura 5.25.

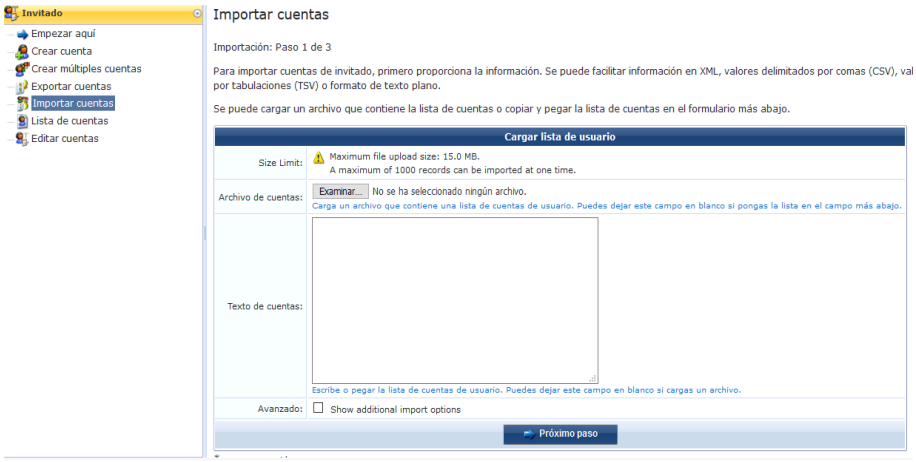


Figura 5.22 Interfaz de gestión usuarios INVITADOS - Importar cuentas.

.

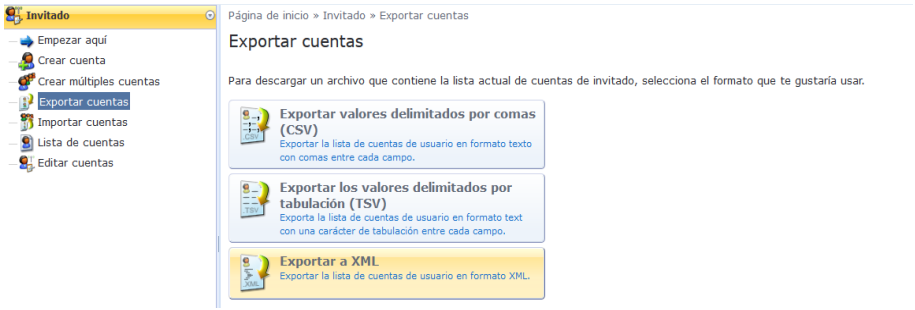


Figura 5.23 Interfaz de gestión usuarios INVITADOS - Exportar cuenta.

.

Figura 5.24 Interfaz de gestión usuarios INVITADOS - Listar cuentas.

.

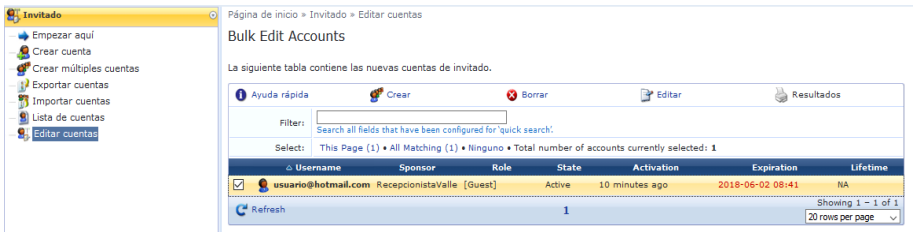


Figura 5.25 Interfaz de gestión usuarios INVITADOS - Editar cuentas.

.

5.6 Instalación de la red

5.6.1 Instalación y sustitución del cableado

- Desmontaje del cableado

  Los enlaces permanentes y latiguillos que se deben actualizar se desmontan y retina para poder instalar el nuevo material.

- Tendido del cableado

  Los cables se tenderán sobre las rutas previstas - habitualmente con una guía de cuerda o varilla. La guía y la unión entre la guía del cable debe ser lo suficientemente fuerte como para aguantar la tensión requerida para situarlo en su localización. La unión entre la guía y el cable debe ser lo más delicado posible para asegurar que no se produzca ningún enganche al tirar por el tendido.

  Durante la tirada del cable se debe evitar todo tipo de estrangulamiento, torceduras, tirones y radios de curvatura inferiores a 5 cm. Durante la instalación del cable se cuidarán los siguientes aspectos:

  – La conexión del cable a tomas y paneles se realiza de acuerdo con los esquemas de conexion T568A.
  – El cableado estructurado debe instalarse según las recomendaciones del fabricante.
  – El radio de curvatura mínimo del cable debe ser respetado, evitando en todo caso radios de curvatura inferiores a 5 cm.
  – Los canales se instalarán paralela o verticalmente a las líneas de intersección entre techo/suelo y paredes.
  – Las canalizaciones no deben ser sobrecargadas.
  – Para la instalación se utilizan los elementos de soporte y fijación que indique el fabricante.
  – Las bridas de fijación deberán permitir el desplazamiento longitudinal de los cables a través de ellas, no estrangulándolos en ningún caso.

  Para la instalación de los tendidos aéreos es imprescindible usar cables con cubiertas resistentes y protección ultravioleta (uv). Es necesario respetar la altura mínima del tendido acorde con el entorno donde se instale (recomendable altura superior a 4,7 mts).

  En el armario del CPD los cables se distribuyen de forma que quede libre el mayor espacio posible en el interior del rack. Se respeta en todo el radio de curvatura de los cables y se incorporan los siguientes elementos interiores:

  – Paneles de 24 tomas RJ45 hembra con características mínimas necesarias para cumplir con Categoría 6A para cuatro pares con o sin pantalla, aportando Clase E al enlace horizontal y 1U, con elementos de etiquetado tanto para las tomas como para el panel.
  – Pasahilos metálicos de 1U.

- Etiquetado
  – Los paneles de parcheo se identifican y etiquetan, así como cada una de sus bocas.
  – Cada uno de los extremos de los enlaces permanentes y latiguillos son identificados y etiquetados.

  Las etiquetas de identificación deberán cumplir los siguientes requisitos:

  – Deberá cuidarse que las etiquetas se coloquen de modo que se acceda a ellas, se lean y se modifiquen con facilidad, si es necesario.
  – Las etiquetas deberán ser resistentes y la identificación deberá permanecer legible toda la vida útil prevista del cableado. No podrán estar escritas a mano.
  – Las etiquetas no deberán verse afectadas por humedad ni manchas cuando se manipulen.

- Las etiquetas empleadas en el exterior u otros entornos agresivos deberán diseñarse para resistir los rigores de dicho entorno.
- Si se realizan cambios (por ejemplo en un panel de parcheo), las etiquetas deberán inspeccionarse para determinar si es necesario actualizar la información recogida en las mismas.

El final de la instalación del cableado estructurado se basa en la certificación del nuevo despliegue mediante la herramienta Fluke midiendo todos los datos que se explican en capítulos anteriores.

5.6.2 Instalación puntos de acceso

El procedimiento para la instalación de los diferentes puntos de acceso es el siguiente:

1. Desempaquetar el punto de acceso.
2. Introducir el cable Ethernet a través de la abertura grande en el soporte.
3. Atornillar el montante de soporte en el lugar previsto de instalación.
4. Conectar el cable Ethernet (para alimentación y conexión a la red), al puerto RJ-45, del punto de acceso.
5. Encajar el punto de acceso en el montante de soporte.

5.6.2.1 Localización real de los puntos de acceso

El cableado estructurado que se instala y la ubicación de los puntos de acceso es representada en las siguientes figuras.

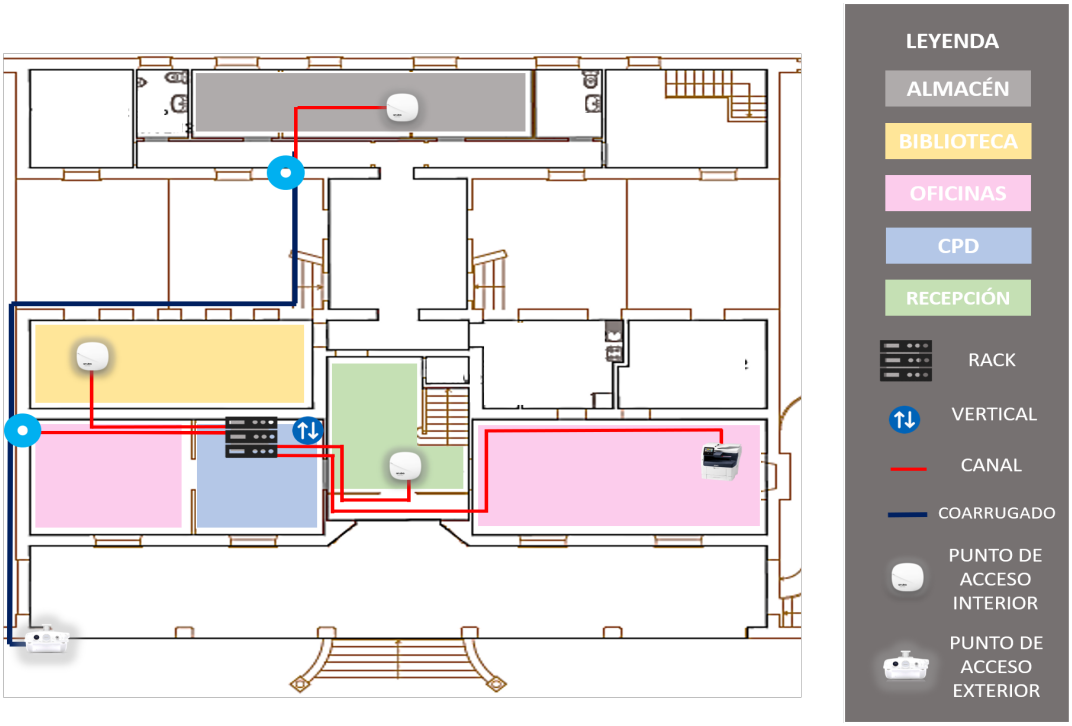


Figura 5.26 Cableado estructurado nuevo de la planta baja.

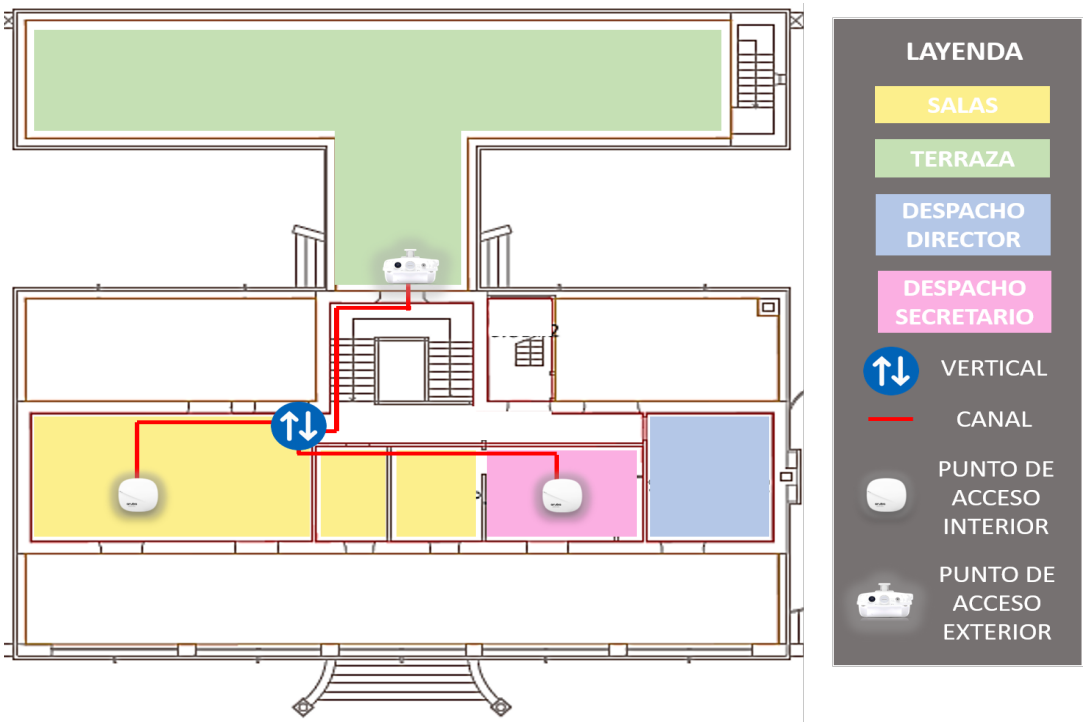


Figura 5.27 Cableado estructurado nuevo de la planta primera.

.

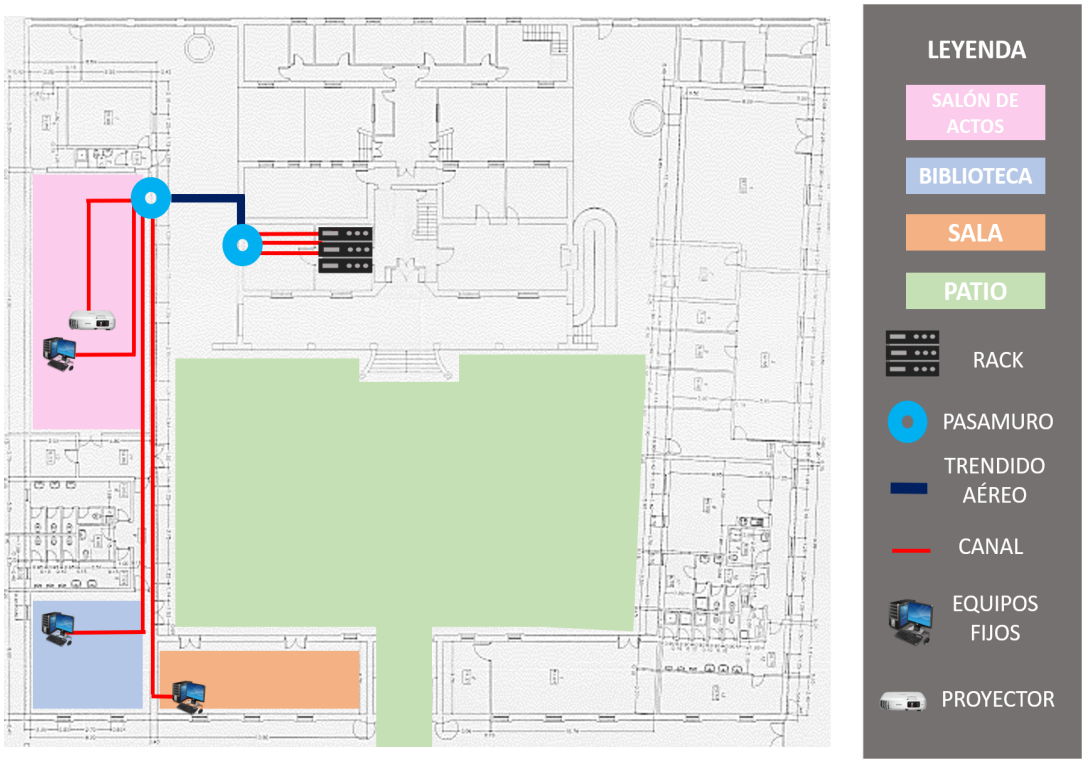


Figura 5.28 Cableado estructurado nuevo de la planta de edificio que envuelven al principal.

.

6 Pruebas y documentación

"1+1=1"

VANESA MARÍA REGALÓN LUQUE

El objetivo de este apartado es documentar el procedimiento con el que se verifica el correcto funcionamiento del despliegue realizado. Las pruebas descritas a continuación están enfocadas a la validación de cada uno de los servicios que se ofrece.

Tabla 6.1 Tabla de pruebas.

Pruebas			
	Servicios Corporativo	Servicios Horizontales	Acceso a Internet
EMPLEADOS	Accesible [B]	Accesible [B]	Accesible [B]
ITINERANTES	No accesible	Accesible [B]	Accesible
INVITADOS	No accesible	No accesible	Accesible [A][B]

Asimismo en la ejecución de las pruebas se verifica el correcto funcionamiento de los siguientes servicios:

- Acceso al portal cautivo. [A]
- Asignación de IP por DHCP en cada pool, así como, el direccionamiento para usuarios locales que es dado por el propio servidor de autenticación.[B]

El acceso a los servicios EMPLEADOS, ITINERANTES e INVITADOS será realizado con usuarios de pruebas provisionales. Para la realización de las pruebas se utiliza un PC y un teléfono móvil con acceso a un navegador (Firefoz, Chrome, IEdge) y conectado a la nueva infraestructura. Usando una de estas aplicaciones, se comprueba llegando a los siguientes resultados.

Tabla 6.2 Tabla de pruebas.

Pruebas				
	Servicios Corporativo	Servicios Horizontales	Acceso a Internet	Direccionamiento
	Carpeta compartida	correo@empresa.com	www.google.es	Local o Centralizado
EMPLEADOS	Accesible	Accesible	Accesible	Local
ITINERANTES	-	Accesible	Accesible	Centralizado
INVITADOS	-	-	Accesible	Centralizado

6.1 Pruebas contra el nodo central

Se lleva a cabo la realización de pruebas sobre los elementos centrales de la Red Corporativa, verificando el correcto funcionamiento de los mecanismos de alta disponibilidad implementados:

- Servidor de autenticación (AAA y Portal Cautivo)

  Verificar que las peticiones RADIUS se envían tanto al servidor RADIUS pasivo como al activo. Respecto al portal cautivo, verificar que el servicio se presta sobre una IP virtual de VRRP.

- Sistema de monitorización central (Gestión y Monitorización)

  Verificar la existencia de conexión SNMP contra el punto de acceso que actúa como controladora virtual.

- Sistema de direccionamiento centralizado (DHCP)

  Verificar que llegan las peticiones de los usuarios ITINERANTES e INVITADOS, y son asignadas del pool correcto de direcciones.

- Controladoras terminadoras de túneles GRE

  Verificar la creación del número de túneles GRE desde el punto de acceso que actúa como controladora virtual hasta ésta, deben ser un total de 5 túneles.

6.2 Pruebas de cobertura

Para el estudio de cobertura real se incluye la siguiente información:

- Elementos hardware de los que se dispone para realizar el estudio: Fluke.
- Elementos software de los que se dispone para realizar el estudio:

  AirMagnet Survey: software utilizado para la asignación, planificación y diseño de las redes LAN inalámbricas 802.11n/a/b/g/ac, calcula la cantidad, colocación y configuración ideales de los puntos de acceso para una implementación exitosa de redes WLAN obteniendo rendimiento y seguridad óptimos.

6.3 Pruebas portal cautivo

Tabla 6.3 Tabla de pruebas portal.

Pruebas	
Redirección automática al portal	OK
Dirección IP del direccionamiento seleccionado para usuarios INVITADOS	OK
Rellenar formulario con correo del sponsor inválido y que produzca error "Debe introducir correo de sponsor válido"	OK
Rellenar formulario con datos sin aceptar términos de uso, provoca el error "Debe aceptar los términos de uso"	OK
Rellenar formulario con datos y pulsar Registrar	OK
Tras el rgistro aparece la pestaña "No cierre esta página, espere que su solicitud sea aprobada"	OK
El correo para la autorización llega al sponsor adeacuado en un tiempo de menos de 1 minuto	OK
El sponsor puede validar correctamente al usuario autorizando el acceso	OK
El usuario pulsa aceptar tras esperar un tiempo no superior a 1 minuto y 30 segundos	OK
El usuario navega por internet	OK
El usuario recibe un email a su cuenta de correo electrónico con las credenciales de la cuenta para que pueda acceder desde otro dispositivo	OK

Tabla 6.4 Tabla de pruebas.

Usuario y contraseña vacíos y provoca "Error debe completar los campos solicitados"	OK
Tras conctarse y desconectar el usuario vuelve a tener conexión si su cuenta no está expirada	OK

6.4 Documentación

En esta documentación tendrá que quedar reflejado:

- Configuración final de los equipos desplegados.
- Documentación de la instalación.
- Descripción y especificaciones técnicas de los elementos instalados.
- Inventario de equipos desplegados.
- Esquemas de red a nivel físico y lógico de la solución.
- Estudio real de cobertura de la solución instalada.
- Diagramas de interconexión con la red existente.
- Resultados obtenidos en el plan de prueba.

7 Presupuesto

"Siempre hay que sumar, nunca restar"

ANTONIA GARCÍA ARJONA

Pruebas			
Descripción	Cantidad	Unitario	TOTAL
WLAN			
Aruba AP-207 Dual 2x2:2 802.11ac AP	8	343,00 €	2.744,00 €
Aruba AP-365 (RW) FIPS/TAA 802.11n/ac Dual 2x2:2 Radio Integrated Omni Ant Outdoor AP	4	1.085,00 €	4.340,00 €
Aruba AP-207 Basic Mount Kit	8	6,59 €	52,72 €
Fijación pared HPE Aruba AP-207	8	13,77 €	110,16 €
Aruba AP-365 Basic Mount Kit	4	9,58 €	38,32 €
Fijación exterior pared HPE Aruba AP-365	4	13,77 €	55,08 €
Licencia HPE Aruba Per AP Capacity	12	25,50 €	306,00 €
Licencia HPE Aruba Per AP PEF	12	25,50 €	306,00 €
Licencia HPE Aruba Per AP RFProtect	12	25,50 €	306,00 €
Colocación e instalación de punto de acceso interior	8	5,50 €	44,00 €
Colocación e instalación de punto de acceso exterior	4	8,00 €	32,00 €
Configuración de arquitectura WLAN y LAN	1	250,00 €	250,00 €
Configuración de arquitectura central	1	200,00 €	200,00 €
Nuevo cableado estructurado			
Suministro e instalación latiguillos con conector macho RJ45 Categoría 6A UTP de 1 metro	24	8,00 €	192,00 €
Suministro e instalación toma de red con conector hembra RJ45 Categoría 6A UTP	12	19,50 €	234,00 €
Suministro e instalación cableado interior (enlace permanente) Categoría 6A UTP de hasta 80 metros.	8	69,60 €	556,80 €
Suministro e instalación cableado Categoría 6A UTP de hasta 80 metros por fachada o exterior	4	96,86 €	387,44 €
Tubo corrugado de hasta Ø25 mm con hilo guía 20 metros	14	2,90 €	40,60 €
Instalación Canaleta PVC de 16 x 30 mm	6	2,54 €	15,24 €
Sustitución cableado estructurado			
Suministro e instalación toma de red con conector hembra RJ45 Categoría 6A UTP	2	11,50 €	23,00 €
Suministro e instalación latiguillos con conector macho RJ45 Categoría 6A UTP de 1 metro	2	8,00 €	16,00 €
Suministro e instalación cableado Categoría 6A UTP de hasta 80 metros.	2	99,60 €	199,20 €
Suministro e instalación latiguillos con conector macho RJ45 Categoría 6A UTP de 1 metro	22	8,00 €	176,00 €
Suministro e instalación de panel de parcheo de 24 puertos UTP RJ-45 de categoría 6A.	1	56,00 €	56,00 €
Ingeniería	1	150,00 €	150,00 €
Replanteo	1	75,00 €	75,00 €
Certificación del cableado estructurado	2	128,00 €	256,00 €
Estudios de cobertura	2	206,30 €	412,60 €
Pruebas y comprobaciones	1	239,50 €	239,50 €
Total			11.813,66 €

8 Aspectos legales

"Que grandes están mis niños"

VALLE SÁNCHEZ DELI

8.1 Cumplimiento del Real Decreto 1066/2001

Para cumplir con los niveles de emisión radioeléctrica recogidos en el R.D. 1066/2001 (BOE Nº234 29/09/2001) y la Orden CTE/23/2002 de 11 de enero de 2002 (BOE Nº11 12/01/2002), se ha de guardar una distancia de seguridad mínima en la dirección de máxima directividad de la antena.
La fórmula utilizada para calcular la distancia de seguridad es la siguiente:

$$D_{max} = \sqrt{\frac{M \cdot P_{pire}}{4 \cdot \pi \cdot S_{max}}} \tag{8.1}$$

$$P_{pire} = P_t \cdot 10^{\frac{G_{ant} - L_{cable}}{10}} \tag{8.2}$$

Significado de los parámetros

P_{pire} →Potencia total transmitida en W.

M → [se tomará 4 como valor más restrictivo]
Es 2,56 si se consideran las condiciones de reflexión,
Es 1 si no se considera reflexión
Es 4 si se considera reflexión total de un rayo

S_{max} → Densidad de potencia máxima permitida del servicio en W/m2.
Para equipos que emiten entre 2 y 300 GHz, el nivel de referencia es de 10 W/m2 (R.D. 1066/2001).

G_{ant} → Ganancia de la antena transmisora.

L_{cable} → Perdida de los cables. Habría que sumar las pérdidas por el splitter en caso de ser usado.

P_t → Potencia de salida en W .

Para obtener el valor más restrictivo de distancia de seguridad, se tomará como PIRE la máxima permitida para cada caso, según la banda de utilización.

8.1.1 Cumplimiento de los niveles de referencia para 2.4 GHz

Según la Nota de utilización nacional UN-85 del CNAF, en la banda de 2.4 GHz el valor máximo de PIRE permitido es de 100 mW. Si se sustituyen los valores en la fórmula de la distancia de seguridad mostrada en el apartado anterior, se obtiene que la distancia de seguridad es de 6 cm.

Tabla 8.1 Datos para el cálculo de la distancia de seguridad 2,4GHz.

.

Calculo distancia de seguridad	
Nivel de referencia	10 (W/m2)
Potencia por canal	100 mW
Número de canales simultáneos	1
P.I.R.E	100 mW
Factor de reflexión	4
Distancia de seguridad	**6 cm**

Los puntos de acceso se instalarán en zonas alejadas de las personas respetando el límite de seguridad.

8.1.2 Cumplimiento de los niveles de referencia para 5 GHz

Según la Nota de utilización nacional UN-128 del CNAF, dentro de esta banda nos podemos encontrar con distintos valores de PIRE según la subbanda utilizada y si son implementadas técnicas de control de potencia (TPC). En el caso del protocolo propietario utilizado por los equipos Alvarion utiliza la subbanda 5470-5725MHz, para esta frecuencia el valor máximo de PIRE permitido es de 1 W, obteniéndose una distancia de seguridad de 18 cm.

Tabla 8.2 Datos para el cálculo de la distancia de seguridad 5GHz.

.

Calculo distancia de seguridad	
Nivel de referencia	10 (W/m2)
Potencia por canal	1 W
Número de canales simultáneos	1
Ganancia de la antena	21 dBi
Pérdidas en los cables	0 dB
P.I.R.E	1 W
Factor de reflexión	4
Distancia de seguridad	**18 cm**

Los puntos de acceso se instalarán en zonas alejadas de las personas respetando el límite de seguridad.

8.2 Cumplimiento de las limitaciones de potencia de los equipos

Las bandas de uso común no son exactamente de libre uso, sino que están reguladas y es de obligado cumplimiento la normativa vigente especificada por la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información (SETSI) en las notas de utilización nacional del Cuadro Nacional de Atribución de Frecuencias (CNAF).

8.3 Políticas de seguridad para redes inalámbricas

En este capítulo se muestra un conjunto de reglas a seguir en la implantación de redes inalámbricas, constituyendo las políticas de seguridad de este tipo de redes. Cada regla lleva asociado un determinado nivel de cumplimiento:

- Obligatorio: su cumplimiento es requisito indispensable para poner en funcionamiento la red. A partir de ahora serán identificadas por una O.
- Recomendable: su cumplimiento es altamente recomendable, en aras de la seguridad de la red inalámbrica. A partir de ahora serán identificadas por una R.

8.3.1 Prevenir el acceso físico a los puntos de acceso

[O] El punto de acceso es el lugar por el que pasan todas las comunicaciones. Para evitar la manipulación de estos es necesario que sean ubicados en lugares apropiados, con acceso restringido y controlado.

Los equipos se instalan en ubicaciones ocultas o elevadas que hacen que no estén al alcance de las personas de paso no autorizadas como los visitantes del parque o los invitados a cualquier evento de los que se lleva a cabo en él.

8.3.2 Restricción del alcance de los puntos de acceso

[O] Restringir el alcance de los puntos de acceso a menores distancias, ya que obliga al atacante a estar físicamente en un lugar controlado por la organización. Para ello se debe comprobar que el límite exterior de la red inalámbrica no quede fuera del perímetro del edificio o de los edificios de la organización, en la medida de lo posible.

Los puntos de acceso que se utilizan en el despliegue disponen de la capacidad de regular su potencia de salida según las necesidades. Estos puntos disponen de una potencia máxima de 100 mW (20 dBm), operando en la banda de 2.4 GHz. Se controlará en cada punto de acceso la potencia de emisión para limitar la cobertura a las zonas deseadas, evitando la propagación de la señal fuera del recinto.

8.3.3 Configuración de los puntos de acceso

[R] Se recomienda deshabilitar todos aquellos protocolos y servicios de los puntos de acceso que no vayan a ser utilizados, siempre que sea posible.

8.3.4 Filtrar direcciones MAC en los puntos de acceso

[R] Con esta medida, se permite que sólo las tarjetas inalámbricas autorizadas puedan acceder a la red, y se evita de esta forma el acceso desde puestos cuya dirección MAC no haya sido dada de alta.

El sistema implementado permite esta posibilidad. Se almacenan todas la MACs que han llegado a realizar peticiones contra el servidor de autenticación RADIUS en un repositorio dedicado para ello. Además, uno de los filtros de autorización existente en el Active Directory de la empresa es el registro de MACs autorizadas por usuario conectado.

8.3.5 Deshabilitación del servidor DHCP en los puntos de acceso

[O] Se recomienda no activar DHCP, u otro protocolo de asignación dinámica de direcciones IP, para evitar que un atacante obtenga una dirección IP de forma sencilla, obligándole a tener que capturar y analizar el tráfico de la red en busca de los parámetros de red utilizados (rango de direcciones IP utilizado, DNS, Gateway, etc.).

El servidor DHCP de los equipos está deshabilitado. De esta tarea se encarga el servidor propio que se encuentra físicamente en la sede y aporta direcciones en el caso del servicio LOCAL. Por otro lado, en el caso del servicio INVITADOS e ITINERANTE el direccionamiento está en el servidor DHCP centralizado.

8.3.6 Nombre del SSID aleatorio o sin relación directa con la organización

[O] El SSID es el nombre por el que se identifica la red inalámbrica. Sin conocer el SSID ni las claves es difícil acceder a una red inalámbrica. Por ello no se deben utilizar nombres relativos a la organización y no deben contener información útil para un atacante. No podrá usarse como SSID de los puntos de acceso el que viene configurado por defecto por los fabricantes.
Existen dos SSID diferentes en esta red, el primero EMPLEADOS, el cual no muestra ninguna relación con la empresa, ni facilita información relevante. Por otro lado, se encuentra el SSID INVITADOS, el cual se basa en facilitar el acceso a los usuarios visitantes. Es abierto.

8.3.7 Uso de algoritmos de cifrado

[O] En ningún caso se podrá instalar una red inalámbrica sin cifrar las comunicaciones. Para cifrar las comunicaciones en el interfaz aéreo se deberá utilizar el algoritmo de cifrado reconocido más avanzado y que proporcione mayor seguridad y garantías, el cual deberá estar recogido o incluido en el estándar de tecnología inalámbrica vigente.

En la red Corporativa que nos comprende se usa algoritmo de encriptación AES de 128 bits. En la red de invitados no aplica al tratarse de una red pública.

8.3.8 Uso de sistemas de autenticación independientes de los puntos de acceso

[O] Se deberán utilizar mecanismos de autenticación acordes a las necesidades de seguridad de la entidad o a la política de seguridad, dado el caso, que ésta tenga establecida, o vaya a establecer en el futuro. Deberán seleccionarse mecanismos de autenticación independientes de los puntos de acceso. Los protocolos que actualmente suelen utilizarse son EAP/TLS y EAP/TTLS o EAP/PEAP.

En el caso de esta red, así como cualquier red que se incorpore a la Red Corporativa en cuestión, utiliza un servidor RADIUS centralizado, con 802.1x para la autenticación, usando EAP-PEAP o EAP-TTLS. La validación de los usuarios se realizará contra una base de datos, Active Directory o LDAP que almacenará los datos de los usuarios autorizados.

8.3.9 Cambios de configuración en los puntos de acceso para su administración

[O] Se deben cambiar de forma obligatoria las contraseñas configuradas por defecto en los puntos de acceso, debiendo utilizar en su lugar otras suficientemente robustas y de acuerdo a la “política de contraseñas”. En caso de tener que realizar un cambio de configuración en un punto de acceso se requerirá que el dispositivo cuente con un control de acceso de usuarios, sea cual sea su método de administración, y en caso de que sea remoto, deberá hacerse utilizando un canal seguro (como por ejemplo SSL).

Los puntos de acceso disponen de control de configuración mediante terminal o acceso Web, usando canales de comunicación seguros (SSH ó HTTPS) para la conexión remota. Además, cada punto de acceso cuenta con un sistema de log donde se almacenan todos los cambios, modificaciones y nuevas configuraciones con un mes de duración.

8.3.10 Copia de seguridad de la configuración de los puntos de acceso y protección de esta

[O] En caso de producirse un reseteo de la configuración del punto de acceso, es muy útil disponer de una copia de toda la configuración. La mayor parte de dispositivos almacenan toda la configuración en archivos que es posible descargar por distintas vías. En estos archivos se almacena información de claves de cifrado y contraseñas de acceso, por lo que es necesario protegerla. Será obligatorio realizar copias de seguridad de la

configuración de los puntos de acceso, con la periodicidad que se haya establecido.

Las copias de seguridad de toda la configuración de los puntos de acceso se llevan a cabo de dos formas:

- Tras cualquier modificación llevada a cabo en un punto de acceso.
- Periódicamente cada mes.

8.3.11 Protocolo de administración en los puntos de acceso

[O] Deberá utilizarse un protocolo de administración de puntos de acceso que disponga de mecanismos robustos de autenticación.

El sistema de administración de los puntos de acceso se realiza mediante el sistema de gestión centralizado, monitorizando de manera proactiva el estado y el rendimiento de todos los puntos de acceso. En este caso no se utiliza necesariamente el protocolo SNMP, de forma que en los puntos de acceso aparece desactivado.

8.3.12 Actualización de firmware sobre los puntos de acceso

[O] Es necesario actualizar los APs a sus últimas versiones de firmware, más aún si las nuevas versiones traen mejoras relativas a la seguridad del protocolo, encriptación de los datos, autenticación de los usuarios o cualquier otra característica.

La versión de los puntos de acceso que se incorporan a la red poseen la última versión existente en el mercado. En desarrollos y mantenimientos futuras, se mantendrán los equipos actualizados con el último firmware disponible siempre y cuando se haya comprobado el buen funcionamiento de este y que además aporte mejoras que sean aplicables a la sede.

8.3.13 Separación entre la red inalámbrica y la red física

[R] Es recomendable la instalación de un cortafuegos entre los puntos de acceso y la LAN, para separar las redes. Asimismo, es recomendable el uso de diferentes VLAN, que distingan entre usuarios inalámbricos y cableados, o bien para poder hacer uso de diferentes perfiles de usuarios inalámbricos.
No aplica en este caso. La sede no cuentan con un firewall entre su arquitectura, es un equipo caro, que, aunque su funcionalidad es necesaria para redes de acceso a internet, en este caso la seguridad se tiene en el nodo central, que es desde donde se accede al exterior. La división en VLAN, para separar el tráfico, no se lleva a cabo por petición del cliente.

8.3.14 Medidas relativas a usuarios INVITADOS

En el caso de establecer el uso de servicio INVITADOS, se deberán tener en cuenta los siguientes requisitos:

- Se llevará un registro de los usuarios “INVITADOS” que se desean conectar a la red inalámbrica, los recursos o servicios a los que accederían y la temporalidad de la conexión, dependiendo esta última de la política de seguridad de la entidad y de las necesidades del usuario.
- Se establecerán los mecanismos necesarios para permitir el acceso de los usuarios de esta red únicamente a los recursos que se considere conveniente proporcionarles, limitando su acceso al resto de recursos de la red.
- Las conexiones de los clientes inalámbricos externos irán convenientemente cifradas.
- Por otro lado, se recomienda que el tráfico de los clientes inalámbricos externos vaya por una VLAN independiente a la de los empleados.

8.4 Normas de cableado estructurado

- ANSI/TIA/EIA-568-B

  Cableado de Telecomunicaciones en Edificios Comerciales sobre como instalar el cableado.

  - TIA/EIA 568-B1: Requerimientos generales
  - TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado
  - TIA/EIA 568-B3: Componentes de cableado, Fibra óptica.

- ANSI/TIA/EIA-569-A

  Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.

- ANSI/TIA/EIA-570-A

  Normas de Infraestructura Residencial de Telecomunicaciones.

- ANSI/TIA/EIA-606-A

  Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.

- ANSI/TIA/EIA-607

  Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

- ANSI/TIA/EIA-758

  Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

9 Conclusiones

9.1 Conclusión profesional

"Quién rompa el cristal, lo paga"

ANTONIO CANO ZAMORA

El proyecto tiene como objetivo la optimización de la comunicación entre las diferentes redes de la empresa, así como la mejora de las prestaciones del usuario, a nivel de seguridad, rendimiento y escalabilidad.

La fase de requisitos recoge todas las necesidades del cliente, no se trata de que intenten justificar el proyecto sino de que expliquen de dónde surgen esas necesidades lo que finalmente desembocan en descubrir cual es el objetivo real del proyecto.

Durante la etapa de análisis se estudia el contexto en el que se encuentra y se contrapone con el que se plantéa examinando el cableado estructurado y la red LAN, así como, realizando un estudio de cobertura inicial de la red WLAN. Tras este análisis las conclusiones a las que se llegan son:

- Sustitución de todos los elementos que no han pasado la certificación, dos enlaces permanentes, dos tomas de red y todos los latiguillos que llegaban a cada uno de los equipos fijos de la red inicial.
- Necesidad de fragmentación y segmentación de la red de forma correcta y ordenada mediante el uso de VLANs.
- Necesidad de 9 puntos de acceso para cubrir las zonas requeridas.

Con la aceptación del cliente sobre las primeras aproximaciones del diseño de la red y las nuevas necesidades que surgen tras su revisión se llega a la fase de diseño, donde se plasman las nuevas ideas y se integran con las ya expuestas y aceptadas. Esto da lugar a un nuevo replanteo que deriva en la necesidad de un total de 12 puntos de acceso que son seleccionados tras un extenso análisis y comparación del equipamiento Wi-Fi existente en el mercado. La elección final reside en el modelo de punto de acceso interior AP-207 y modelo exterior AP-365, ambos de Aruba HP, seleccionando la arquitectura con controladora virtual (VC).

En el bloque de cableado estructura se suministra un nuevo canal completo de Cat6A para cada nuevo punto de acceso con sus correspondientes canaletas.

La red LAN se divide teniendo en cuenta la gestión de usuarios que son clasificados según la conmutación de su tráfico y los accesos con los que cuentan:

- EMPLEADOS

  Usuarios que se conectan al servicio WI-Fi, son empleados de la sede, con conmutación del tráfico a nivel 2, direccionamiento del DHCP local y acceso a los recursos locales, los servicios horizontales y a Internet.

- ITINERANTES

  Usuarios que se conectan al servicio WI-Fi, son empleados de la empresa, pero no de la sede, con conmutación del tráfico centralizada a nivel 2 en las terminadoras de túneles hacia la VPN ITINERANTE, direccionamiento del DHCP centralizado y acceso a los servicios horizontales y a Internet.

- INVITADOS

  Usuarios que se conectan al servicio WI-Fi, y son visitantes. Dicho acceso será de carácter temporal, con conmutación del tráfico centralizada a nivel 2 en las terminadoras de túneles hacia la VPN INTERNET, direccionamiento del DHCP centralizado y acceso a Internet.

Las conexiones de los usuarios a la red WLAN se llevan a cabo mediante dos SSID diferentes, uno EMPLEADOS (LOCAL e ITINERANTES) y otra INVITADOS. Para porder hacer frente a la clasificación anterior la red LAN es fragmentada en cinco VLANs:

- VLAN CONTROL

  Esta VLAN es utilizada para la gestión de los puntos de acceso, su configuración y posterior seguimiento.

- VLAN FIJOS

  Esta VLAN es utilizada para el tráfico de los equipos fijos, la impresora y el proyector.

- VLAN LOCAL

  Esta VLAN es utilizada para el tráfico de los usuarios WI-Fi inalámbricos.

- VLAN ITINERANTES

  Esta VLAN es utilizada para el tráfico de los usuarios ITINERANTES.

- VLAN INVITADOS

  Esta VLAN es utilizada para el tráfico de los usuarios INVITADOS.

Desde el punto de vista de los servicios requeridos para poder autenticar y autorizar correctamente a los usuarios se divide en dos servicios con autenticación 802.1x que autentican contra el servidor RADIUS centralizado, uno por cada SSID.

- Servicio EMPLEADOS

  La fuente de autentización será tanto el Active Directory, como la BBDD local del servidor RADIUS. Si el usuario que pertenece al grupo Sede-central del ActiveDirectory y pertenezca al grupo de puntos de acceso llamado Sede20, se le asigna el rol LOCAL, mientras que aquel usuario que no cumple la condición anterior, se le asigna el rol ITINERANTE.

- Servicio INVITADOS

  La fuente de autentización será la BBDD local de usuarios invitados del servidor RADIUS. El usuario tendrá que pasar un portal cautivo con un formulario que le solicita sus datos personales, y tras la validación de esta cuenta por parte del sponsor se le asigna el rol INVITADOS.

Cada rol corresponde con unas políticas y unas restricciones que le otorga a cada uno de los usuarios los accesos que se han comentado anteriormente.

Tras la implantación, la sede se encuentra integrada en la Red Corporativa y funcionando al máximo rendimiento gracias a la solución óptima que cumple con todos los requisitos y necesidades con las que contaba la

sede. El sistema es muy flexible y escalable por lo que se podrá ampliar si así se necesita en un futuro, tanto en velocidad como en cobertura o en un aumento de número de usuarios o accesos. Incluso sería interesante la implantación por todo el parque necesitando una mayor cantidad de puntos de acceso exterior.

Bibliografía

"Hazle dos huevos fritos"

ÁNGEL NARANJO ÁLVAREZ

- http://www.flukenetworks.com/
- http://www.arubanetworks.com/
- http://www.cisco.com
- http://www1.frm.utn.edu.ar/medidase2/varios/parametros-redes1.pdf
- http://www.gonzalonazareno.org/certired/p15f/p15f.html
- http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43922/10/jgarciamolinTFC0715memoria.pdf
- http://matematicas.uclm.es/earanda/wp-content/uploads/downloads/2013/10/latex.pdf
- https://community.arubanetworks.com/
- https://www.arubanetworks.com/products/networking/aruba-instant/instant-training/
- Redes telemáticas - Carlos Valdivia Miranda

Glosario

- AP: Access Point (Punto de Acceso).
- CPD: Centro de Procesamiento de Datos y hace referencia a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- DHCP: Dynamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Equipos. Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. HTTP: Hyper Terminal Transfer Protocol
- EAP: Extensible Authentication Protocol o Protocolo de Autenticación Extensible es un framework de autenticación utilizado habitualmente en redes WLAN punto a punto.
- IEEE: Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos. Es la asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo de áreas técnicas.
- IP: Internet Protocol o Protocolo de Internet. Es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI.
- ICMP: Internet Control Message Protocol o Protocolo de Mensajes de Control de Internet. Es un sub protocolo de control y notificación de errores del protocolo IP. IPSEC: Internet Protocol Security
- LAN: Local Area Network o Red de Área Local. Es una red de comunicaciones que abarca un área reducida.
- MAC: Media Control Access o Control de Acceso al Medio. La subcapa MAC se sitúa en la capa de enlace de datos y es responsable, entre otras cosas, de controlar el acceso al medio físico de transmisión por parte de los dispositivos que comparten el mismo canal de comunicación.
- MIMO: Multiple Input Multiple Output (Múltiple entrada múltiple salida), se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos.
- NAT: Network Address Translation
- PIRE: Potencia Isotrópica Radiada Equivalente
- PoE: Power over Ethernet
- PSK: Pre Shared Key
- QoS: Quality of Service
- Radius: Remote Authentication Dial-In User Service o Servicio de Autenticacón de Usuarios Remotos. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
- RF: Radio Frequency
- RFC: Request for Comments
- SFP: Small Form-Factor Pluggable Transceiver

- SNMP: Simple Network Management Protocol o Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- SNR: Signal to noise. La relación señal/ruido se define como el margen que hay entre la potencia de la señal que se transmite y la potencia del ruido que la corrompe.
- SSID: Service Set Identifier
- STP: Spanning Tree Protocol
- Switch: Conmutador.
- TCP: Protocolo de Control de Transmisión.
- Throughput o rendimiento: Cantidad de datos por unidad de tiempo que fluyen por un sistema.
- UDP: Protocolo de Datagramas de Usuario.
- UTP: Unshielded twisted pair o Par Trenzado sin Apantallar. Es un tipo de cable de par trenzado que no se encuentra blindado y que se utiliza principalmente para comunicaciones debido a flexibilidad y bajo costo.
- VLAN: Virtual Local Area Network
- VPN: Virtual Private Network
- WEP: Wired Equivalent Privacy o Privacidad Equivalente a un Medio Cableado. Es un sistema de cifrado incluido en el estándar 802.11 como protocolo para las redes Wireless que permite cifrar la información que se transmite.
- WLAN: Wireless LAN o Red de Área Local Inalámbrica. Es un sistema de comunicación inalámbrica flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas.
- WPA: Wi-Fi Protected Access o Acceso Protegido Wi-Fi. Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo, WEP.

Anexos

1 DATA SHIFT ARUBA 207

https://www.arubanetworks.com/assets/ds/DSAP207Series.pdf

2 DATA SHIFT ARUBA 365

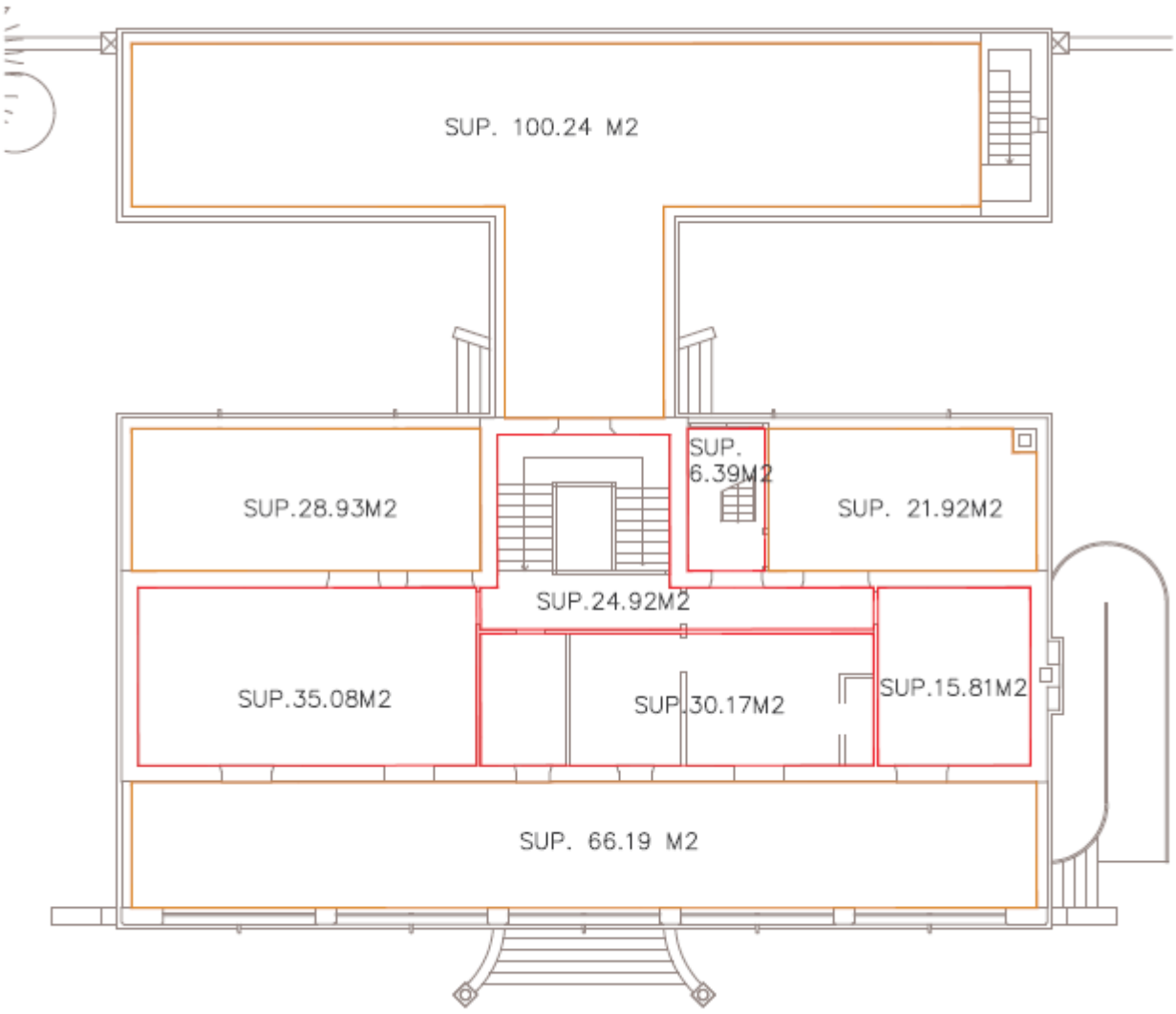
https://www.arubanetworks.com/assets/ds/DSAP360Series.pdf

3 Instalación punto de acceso exterior

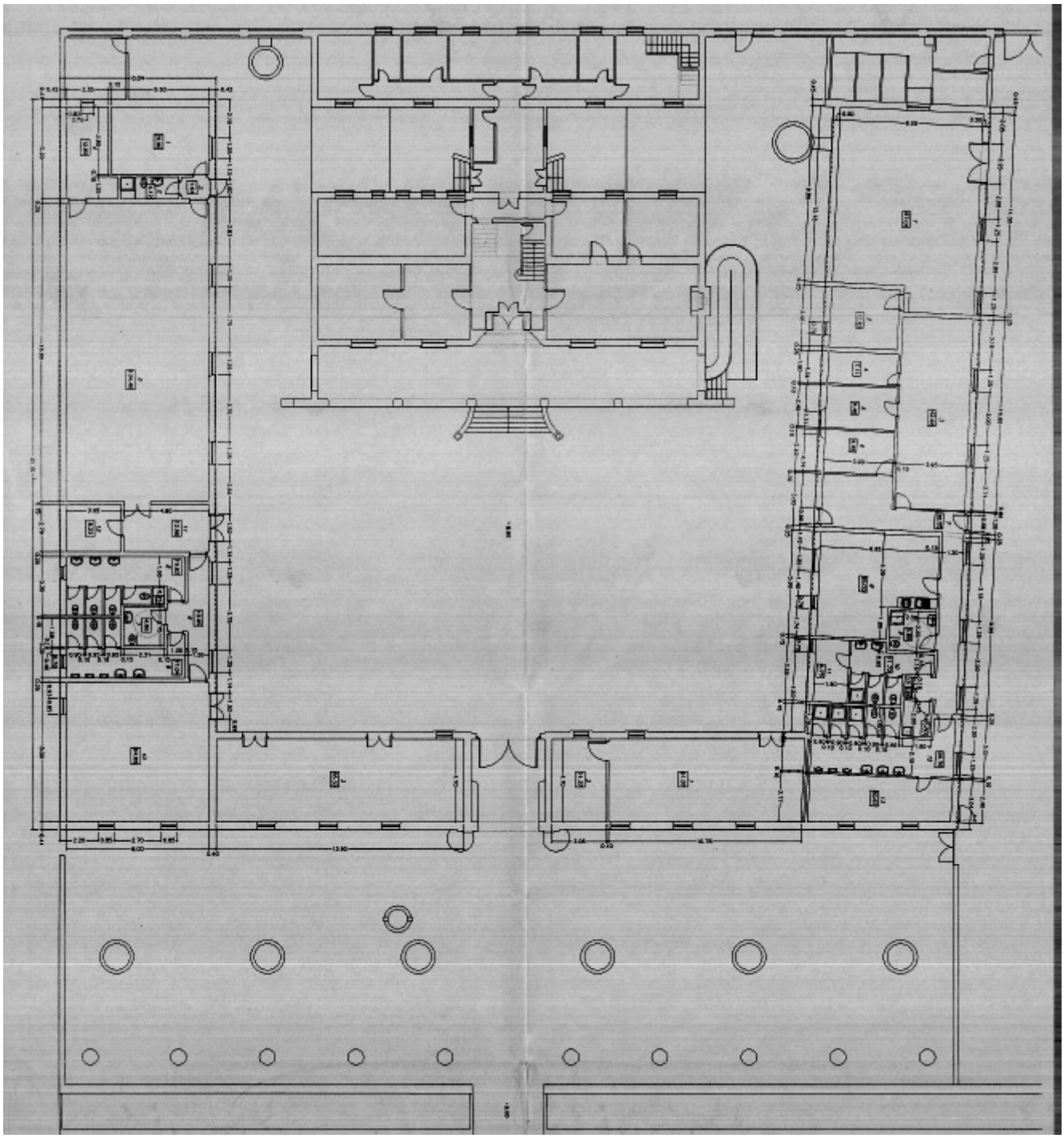
https://support.hpe.com/hpsc/doc/public/display?docId=emrna-a00036501enusdocLocale=enUS

4 Plano planta baja

5 Plano planta primera



6 Plano planta baja y anexos



7 Certificación Fluke cableado final

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-2 **PASA***

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.2 dB
12/30/2017 09:29 AM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 36, 250.0 MHz	PASA	6.4	31.1	24.7
NEXT (dB)	Par 12-36, 84.0 MHz	PASA	44.3	43.1	1.2
PS NEXT (dB)	Par 36, 237.0 MHz	PASA*	34.1	33.1	1.0
ACR-N (dB)	Par 12-36, 3.4 MHz		70.0	61.8	8.2
PS ACR-N (dB)	Par 12, 3.9 MHz		68.9	58.5	10.4
ACR-F (dB)	Par 45-36, 250.0 MHz	PASA	30.0	16.2	13.8
PS ACR-F (dB)	Par 36, 1.0 MHz	PASA	73.8	61.2	12.6
RL (dB)	Par 36, 210.0 MHz	PASA	15.3	10.8	4.5
Longitud (m)	Par 78	PASA	17.4	90.0	72.6
Tiempo de Prop. (ns)	Par 36	PASA	87	498	411
Diferencia Retardo (ns)	Par 36	PASA	3	44	41
Resistencia (ohms)	Par 36		3.0		
Mapa de Cableado		PASA			

ID. Cable: AP-3 **PASA**

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.8 dB
12/30/2017 09:31 AM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 36, 250.0 MHz	PASA	5.2	31.1	25.9
NEXT (dB)	Par 12-36, 240.5 MHz	PASA	37.4	35.6	1.8
PS NEXT (dB)	Par 36, 250.0 MHz	PASA	33.9	32.7	1.2
ACR-N (dB)	Par 12-36, 10.1 MHz		66.1	52.2	13.9
PS ACR-N (dB)	Par 36, 11.5 MHz		63.4	48.6	14.8
ACR-F (dB)	Par 36-78, 3.5 MHz	PASA	66.1	53.3	12.8
PS ACR-F (dB)	Par 36, 1.0 MHz	PASA	72.1	61.2	10.9
RL (dB)	Par 45, 199.5 MHz	PASA	15.6	11.0	4.6
Longitud (m)	Par 78	PASA	14.1	90.0	75.9
Tiempo de Prop. (ns)	Par 36	PASA	70	498	428
Diferencia Retardo (ns)	Par 36	PASA	2	44	42
Resistencia (ohms)	Par 36		2.3		
Mapa de Cableado		PASA			

ID. Cable: AP-1 **PASA***

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 0.9 dB
12/30/2017 10:18 AM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 36, 250.0 MHz	PASA	2.8	31.1	28.3
NEXT (dB)	Par 36-78, 248.0 MHz	PASA*	36.3	35.4	0.9
PS NEXT (dB)	Par 36, 246.5 MHz	PASA*	33.8	32.8	1.0
ACR-N (dB)	Par 45-78, 8.1 MHz		67.6	54.3	13.3
PS ACR-N (dB)	Par 45, 8.3 MHz		65.7	51.8	13.9
ACR-F (dB)	Par 36-78, 3.3 MHz	PASA	66.3	54.0	12.3
PS ACR-F (dB)	Par 36, 1.0 MHz	PASA	72.4	61.2	11.2
RL (dB)	Par 36, 107.5 MHz		14.6	13.7	0.9
Longitud (m)	Par 12	PASA	6.6	90.0	83.4
Tiempo de Prop. (ns)	Par 36	PASA	33	498	465
Diferencia Retardo (ns)	Par 36	PASA	1	44	43
Resistencia (ohms)	Par 36		1.1		
Mapa de Cableado		PASA			

ID. Cable: AP-9 **PASA**

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.9 dB
12/30/2017 10:47 AM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	8.0	31.1	23.1
NEXT (dB)	Par 12-36, 235.0 MHz	PASA	37.7	35.8	1.9
PS NEXT (dB)	Par 36, 240.0 MHz	PASA	34.6	33.0	1.6
ACR-N (dB)	Par 36-45, 7.1 MHz		64.4	55.5	8.9
PS ACR-N (dB)	Par 36, 6.9 MHz		62.1	53.5	8.6
ACR-F (dB)	Par 36-45, 2.6 MHz	PASA	65.8	55.8	10.0
PS ACR-F (dB)	Par 36, 2.4 MHz	PASA	65.9	53.7	12.2
RL (dB)	Par 12, 50.3 MHz	PASA	19.4	17.0	2.4
Longitud (m)	Par 45	PASA	22.3	90.0	67.7
Tiempo de Prop. (ns)	Par 12	PASA	114	498	384
Diferencia Retardo (ns)	Par 12	PASA	6	44	38
Resistencia (ohms)	Par 12		3.6		
Mapa de Cableado		PASA			

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-8

PASA

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.6 dB
12/30/2017 12:08 PM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	15.6	31.1	15.5
NEXT (dB)	Par 36-45, 71.3 MHz	PASA	45.8	44.2	1.6
PS NEXT (dB)	Par 36, 239.5 MHz	PASA	35.3	33.0	2.3
ACR-N (dB)	Par 12-78, 19.3 MHz		53.7	45.6	8.1
PS ACR-N (dB)	Par 36, 10.9 MHz		57.9	49.1	8.8
ACR-F (dB)	Par 45-36, 98.0 MHz	PASA	34.7	24.4	10.3
PS ACR-F (dB)	Par 36, 250.0 MHz	PASA	25.1	13.2	11.9
RL (dB)	Par 12, 9.9 MHz	PASA	22.9	21.0	1.9
Longitud (m)	Par 45	PASA	43.0	90.0	47.0
Tiempo de Prop. (ns)	Par 12	PASA	220	498	278
Diferencia Retardo (ns)	Par 12	PASA	12	44	32
Resistencia (ohms)	Par 36		6.6		
Mapa de Cableado		PASA			

ID. Cable: AP-7

PASA*

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 0.2 dB
12/30/2017 12:55 PM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	24.2	31.1	6.9
NEXT (dB)	Par 36-45, 38.0 MHz	PASA*	48.8	48.6	0.2
PS NEXT (dB)	Par 36, 235.0 MHz	PASA	34.6	33.2	1.4
ACR-N (dB)	Par 36-45, 38.0 MHz		40.5	37.6	2.9
PS ACR-N (dB)	Par 36, 38.0 MHz		39.7	35.1	4.6
ACR-F (dB)	Par 45-36, 204.0 MHz	PASA	28.3	18.0	10.3
PS ACR-F (dB)	Par 36, 187.0 MHz	PASA	27.4	15.8	11.6
RL (dB)	Par 12, 6.4 MHz	PASA*	22.0	21.0	1.0
Longitud (m)	Par 45	PASA	67.2	90.0	22.8
Tiempo de Prop. (ns)	Par 12	PASA	344	498	154
Diferencia Retardo (ns)	Par 12	PASA	19	44	25
Resistencia (ohms)	Par 12		10.6		
Mapa de Cableado		PASA			

ID. Cable: AP-6

PASA

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.7 dB
12/30/2017 12:57 PM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	25.1	31.1	6.0
NEXT (dB)	Par 12-36, 246.5 MHz	PASA	37.1	35.4	1.7
PS NEXT (dB)	Par 36, 245.0 MHz	PASA	34.4	32.9	1.5
ACR-N (dB)	Par 36-45, 35.8 MHz		43.0	38.3	4.7
PS ACR-N (dB)	Par 36, 16.5 MHz		50.4	44.9	5.5
ACR-F (dB)	Par 45-36, 187.0 MHz	PASA	28.4	18.8	9.6
PS ACR-F (dB)	Par 36, 1.0 MHz	PASA	71.7	61.2	10.5
RL (dB)	Par 12, 10.3 MHz	PASA	22.2	20.9	1.3
Longitud (m)	Par 45	PASA	69.7	90.0	20.3
Tiempo de Prop. (ns)	Par 12	PASA	357	498	141
Diferencia Retardo (ns)	Par 12	PASA	20	44	24
Resistencia (ohms)	Par 12		10.9		
Mapa de Cableado		PASA			

ID. Cable: AP-4

PASA

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.3 dB
01/02/2018 12:54 PM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	26.1	31.1	5.0
NEXT (dB)	Par 36-45, 82.5 MHz	PASA	44.5	43.2	1.3
PS NEXT (dB)	Par 36, 235.0 MHz	PASA	35.4	33.2	2.2
ACR-N (dB)	Par 36-45, 19.3 MHz		48.6	45.6	3.0
PS ACR-N (dB)	Par 36, 19.3 MHz		47.9	43.2	4.7
ACR-F (dB)	Par 45-36, 168.0 MHz	PASA	30.5	19.7	10.8
PS ACR-F (dB)	Par 36, 1.0 MHz	PASA	72.1	61.2	10.9
RL (dB)	Par 12, 8.4 MHz	PASA	22.7	21.0	1.7
Longitud (m)	Par 45	PASA	72.8	90.0	17.2
Tiempo de Prop. (ns)	Par 12	PASA	373	498	125
Diferencia Retardo (ns)	Par 12	PASA	21	44	23
Resistencia (ohms)	Par 12		11.3		
Mapa de Cableado		PASA			

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-5 **PASA***

Cat 6 U/UTP | TIA Cat 6 Perm. Link | Paso Libre (NEXT): 1.2 dB
01/02/2018 01:19 PM | DTX-1800 | N/S: 9126090

Pruebas	Detallado	Estado	Valor	Límite	Margen
Pérdida inserción (dB)	Par 12, 250.0 MHz	PASA	23.6	31.1	7.5
NEXT (dB)	Par 36-45, 250.0 MHz	PASA	36.5	35.3	1.2
PS NEXT (dB)	Par 36, 250.0 MHz	PASA*	33.5	32.7	0.8
ACR-N (dB)	Par 12-78, 11.0 MHz		56.2	51.4	4.8
PS ACR-N (dB)	Par 78, 11.0 MHz		55.3	49.0	6.3
ACR-F (dB)	Par 45-36, 212.0 MHz	PASA	25.8	17.7	8.1
PS ACR-F (dB)	Par 36, 187.0 MHz	PASA	26.1	15.8	10.3
RL (dB)	Par 12, 8.0 MHz	PASA	22.4	21.0	1.4
Longitud (m)	Par 45	PASA	65.4	90.0	24.6
Tiempo de Prop. (ns)	Par 12	PASA	335	498	163
Diferencia Retardo (ns)	Par 12	PASA	19	44	25
Resistencia (ohms)	Par 12		10.4		
Mapa de Cableado		PASA			

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

Longitud Total:	378.5 m
Cantidad de Informes:	9
Cantidad de informes de paso:	9
Cantidad de informes de falla:	0
Numero de Advertencias de Reportes:	0
Documentacion Solamente:	0

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-2

Fecha / Hora: 12/30/2017 09:29:26 AM
Paso Libre 1.2 dB (NEXT 12-36)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 78]	17.4
Tiempo de Prop. (ns), Lím. 498	[Par 36]	87
Diferencia Retardo (ns), Lím. 44	[Par 36]	3
Resistencia (ohm.)	[Par 36]	3.0
Pérdida inserción Margen (dB)	[Par 36]	24.7
Frecuencia (MHz)	[Par 36]	250.0
Límite (dB)	[Par 36]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	12-36	12-36	12-36	36-45
NEXT (dB)	1.7	1.2	1.7	3.4
Frec. (MHz)	243.0	84.0	243.0	249.0
Límite (dB)	35.5	43.1	35.5	35.4
Peor Par	36	36	36	36
PS NEXT (dB)	1.0*	2.9	1.1	2.9
Frec. (MHz)	237.0	242.5	243.5	242.5
Límite (dB)	33.1	32.9	32.9	32.9

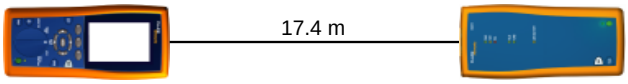
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	36-45	45-36	36-45
ACR-F (dB)	13.8	14.1	13.8	14.1
Frec. (MHz)	250.0	250.0	250.0	250.0
Límite (dB)	16.2	16.2	16.2	16.2
Peor Par	36	36	36	36
PS ACR-F (dB)	12.6	12.7	14.3	15.2
Frec. (MHz)	1.0	1.0	250.0	247.0
Límite (dB)	61.2	61.2	13.2	13.3

N/A	MAIN	SR	MAIN	SR
Peor Par	12-36	12-36	12-36	36-45
ACR-N (dB)	8.2	8.2	26.2	28.4
Frec. (MHz)	3.4	3.4	243.0	249.0
Límite (dB)	61.8	61.8	4.9	4.3
Peor Par	12	12	36	36
PS ACR-N (dB)	10.7	10.4	25.5	27.3
Frec. (MHz)	3.8	3.9	243.5	242.5
Límite (dB)	58.6	58.5	2.3	2.4

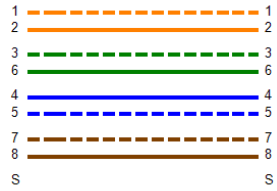
PASA	MAIN	SR	MAIN	SR
Peor Par	36	78	36	78
RL (dB)	4.5	6.8	4.5	6.8
Frec. (MHz)	210.0	187.0	210.0	187.0
Límite (dB)	10.8	11.3	10.8	11.3

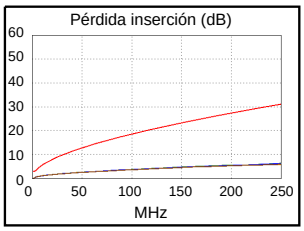
Estándares de Red Compatibles:

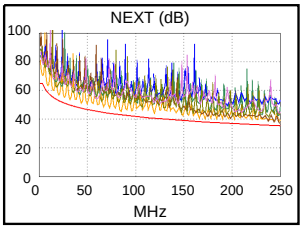
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

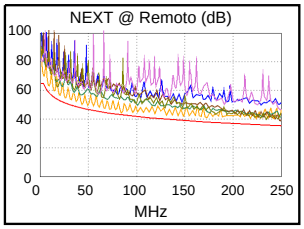


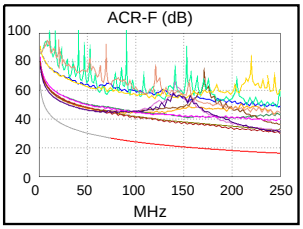
Mapa de Cableado (T568B)
PASA

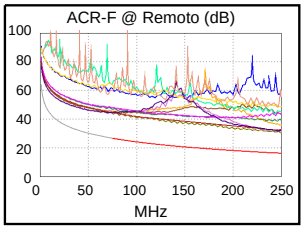


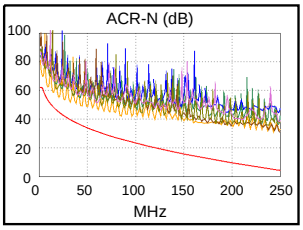


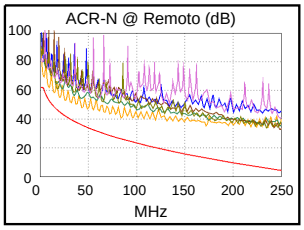


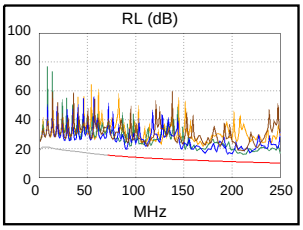


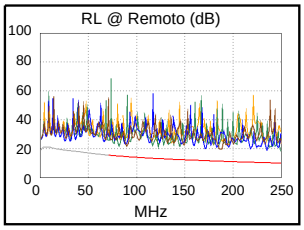












* El margen está dentro de los límites de exactitud del instrumento.

LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-3

Fecha / Hora: 12/30/2017 09:31:02 AM
Paso Libre 1.8 dB (NEXT 12-36)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 78]	14.1
Tiempo de Prop. (ns), Lím. 498	[Par 36]	70
Diferencia Retardo (ns), Lím. 44	[Par 36]	2
Resistencia (ohm.)	[Par 36]	2.3
Pérdida inserción Margen (dB)	[Par 36]	25.9
Frecuencia (MHz)	[Par 36]	250.0
Límite (dB)	[Par 36]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	12-36	12-36	12-36	12-36
NEXT (dB)	1.8	2.3	1.8	2.3
Frec. (MHz)	240.5	240.0	240.5	240.0
Límite (dB)	35.6	35.6	35.6	35.6
Peor Par	36	36	36	36
PS NEXT (dB)	1.2	4.0	1.2	4.0
Frec. (MHz)	250.0	240.5	250.0	240.5
Límite (dB)	32.7	33.0	32.7	33.0

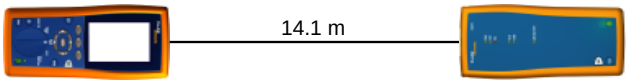
PASA	MAIN	SR	MAIN	SR
Peor Par	36-78	36-78	36-45	45-36
ACR-F (dB)	12.8	12.8	15.5	15.5
Frec. (MHz)	3.5	5.3	248.5	248.5
Límite (dB)	53.3	49.8	16.3	16.3
Peor Par	36	36	36	36
PS ACR-F (dB)	10.9	10.9	16.1	15.9
Frec. (MHz)	1.0	1.0	249.0	248.5
Límite (dB)	61.2	61.2	13.3	13.3

N/A	MAIN	SR	MAIN	SR
Peor Par	12-36	12-36	12-36	12-36
ACR-N (dB)	13.9	14.4	27.2	27.6
Frec. (MHz)	10.1	10.5	240.5	240.0
Límite (dB)	52.2	51.8	5.2	5.3
Peor Par	36	36	36	36
PS ACR-N (dB)	14.8	15.3	27.1	29.4
Frec. (MHz)	11.5	9.9	250.0	240.5
Límite (dB)	48.6	50.1	1.6	2.6

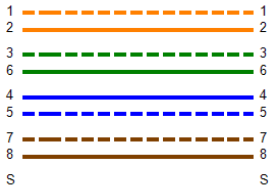
PASA	MAIN	SR	MAIN	SR
Peor Par	45	12	45	45
RL (dB)	4.6	6.4	4.6	7.4
Frec. (MHz)	199.5	121.5	199.5	215.0
Límite (dB)	11.0	13.2	11.0	10.7

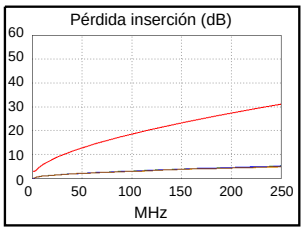
Estándares de Red Compatibles:

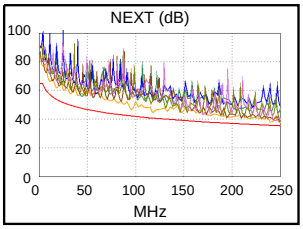
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

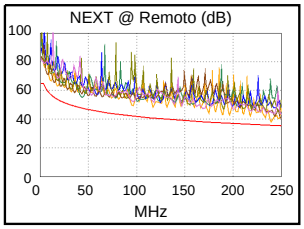


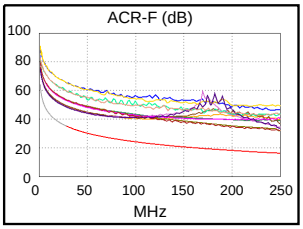
Mapa de Cableado (T568B)
PASA

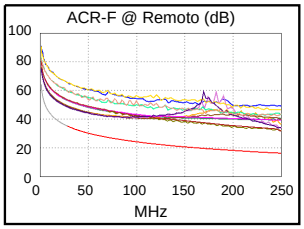


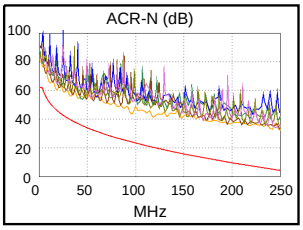


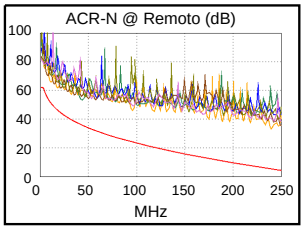


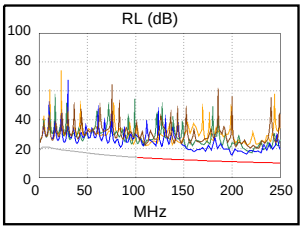


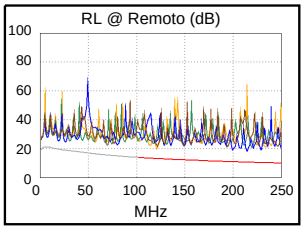












LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-1

Fecha / Hora: 12/30/2017 10:18:07 AM
Paso Libre 0.9 dB (NEXT 36-78)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 12]	6.6
Tiempo de Prop. (ns), Lím. 498	[Par 36]	33
Diferencia Retardo (ns), Lím. 44	[Par 36]	1
Resistencia (ohm.)	[Par 36]	1.1
Pérdida inserción Margen (dB)	[Par 36]	28.3
Frecuencia (MHz)	[Par 36]	250.0
Límite (dB)	[Par 36]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-78	36-45	36-78	36-45
NEXT (dB)	0.9*	1.7	0.9	1.7
Frec. (MHz)	248.0	245.0	248.0	245.0
Límite (dB)	35.4	35.5	35.4	35.5
Peor Par	36	36	36	36
PS NEXT (dB)	1.0*	1.1	1.0	1.1
Frec. (MHz)	246.5	246.0	246.5	246.0
Límite (dB)	32.8	32.8	32.8	32.8

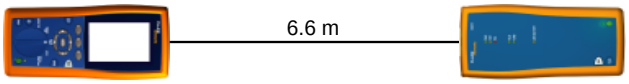
PASA	MAIN	SR	MAIN	SR
Peor Par	36-78	78-36	45-36	36-45
ACR-F (dB)	12.3	12.3	15.2	15.3
Frec. (MHz)	3.3	3.0	249.0	249.0
Límite (dB)	54.0	54.6	16.3	16.3
Peor Par	36	36	36	45
PS ACR-F (dB)	11.2	11.2	15.6	16.3
Frec. (MHz)	1.0	1.0	250.0	249.0
Límite (dB)	61.2	61.2	13.2	13.3

N/A	MAIN	SR	MAIN	SR
Peor Par	45-78	45-78	36-78	36-45
ACR-N (dB)	13.3	13.9	29.3	29.8
Frec. (MHz)	8.1	7.1	248.0	245.0
Límite (dB)	54.3	55.5	4.4	4.7
Peor Par	45	45	36	36
PS ACR-N (dB)	13.9	14.6	29.1	29.2
Frec. (MHz)	8.3	5.9	246.5	246.0
Límite (dB)	51.8	54.9	2.0	2.0

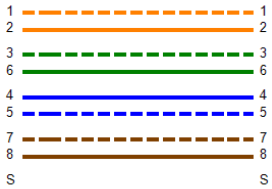
N/A	MAIN	SR	MAIN	SR
Peor Par	36	36	36	36
RL (dB)	0.9	2.2	1.0	2.3
Frec. (MHz)	107.5	47.0	157.5	129.0
Límite (dB)	13.7	17.3	12.0	12.9

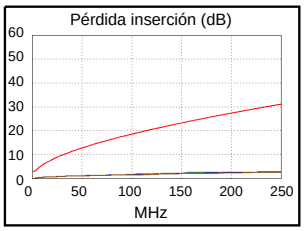
Estándares de Red Compatibles:

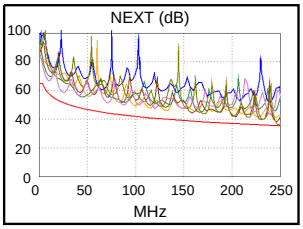
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

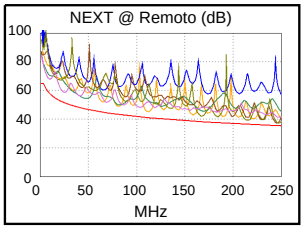


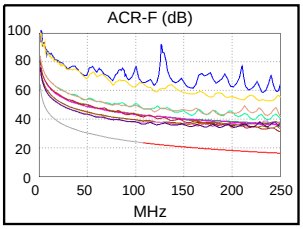
Mapa de Cableado (T568B)
PASA

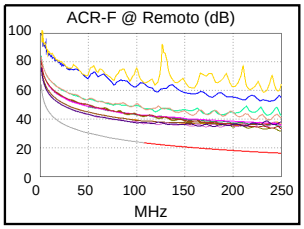


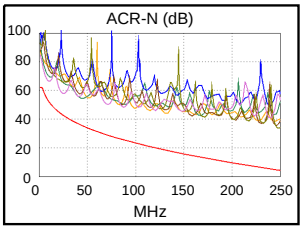


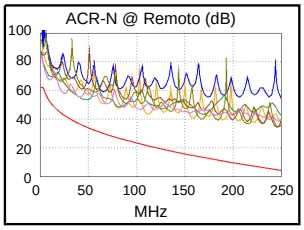


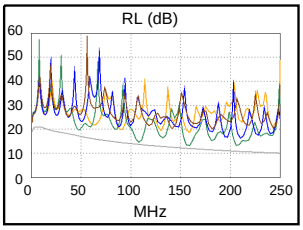


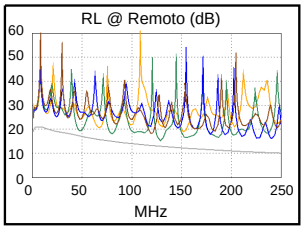












* El margen está dentro de los límites de exactitud del instrumento.

LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-9

Fecha / Hora: 12/30/2017 10:47:54 AM
Paso Libre 1.9 dB (NEXT 12-36)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-CHA002

Longitud (m), Lím. 90.0	[Par 45]	22.3
Tiempo de Prop. (ns), Lím. 498	[Par 12]	114
Diferencia Retardo (ns), Lím. 44	[Par 12]	6
Resistencia (ohm.)	[Par 12]	3.6
Pérdida inserción Margen (dB)	[Par 12]	23.1
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	12-36	12-36	12-36	36-45
NEXT (dB)	1.9	4.3	1.9	4.8
Frec. (MHz)	235.0	74.0	235.0	159.0
Límite (dB)	35.8	44.0	35.8	38.6
Peor Par	36	36	36	36
PS NEXT (dB)	1.6	5.0	1.6	8.2
Frec. (MHz)	240.0	74.0	240.0	200.0
Límite (dB)	33.0	41.5	33.0	34.3

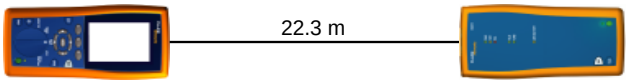
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	45-36	45-36	36-45
ACR-F (dB)	10.0	10.0	15.4	15.8
Frec. (MHz)	2.6	2.5	240.5	240.5
Límite (dB)	55.8	56.2	16.6	16.6
Peor Par	36	36	36	36
PS ACR-F (dB)	12.5	12.2	15.9	17.7
Frec. (MHz)	2.4	2.4	244.5	242.0
Límite (dB)	53.7	53.7	13.4	13.5

N/A	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	12-36	36-45
ACR-N (dB)	8.9	11.4	24.3	27.6
Frec. (MHz)	7.1	6.3	235.0	200.5
Límite (dB)	55.5	56.7	5.8	9.5
Peor Par	36	36	36	36
PS ACR-N (dB)	8.6	12.7	24.4	28.6
Frec. (MHz)	6.9	6.4	240.0	200.0
Límite (dB)	53.5	54.2	2.6	7.0

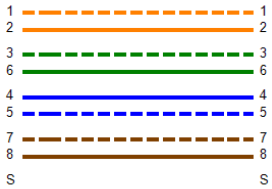
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	45	36
RL (dB)	2.4	2.7	7.6	6.3
Frec. (MHz)	50.3	50.5	235.5	224.0
Límite (dB)	17.0	17.0	10.3	10.5

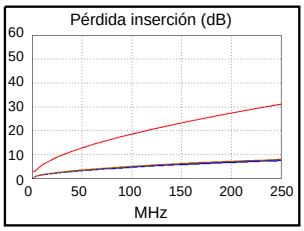
Estándares de Red Compatibles:

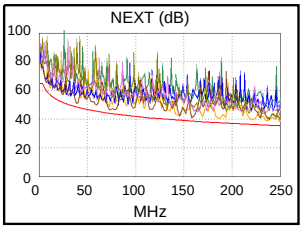
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

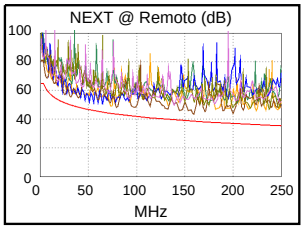


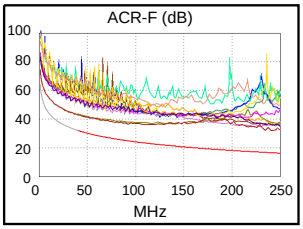
Mapa de Cableado (T568B)
PASA

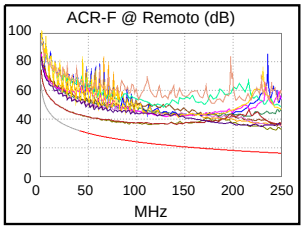


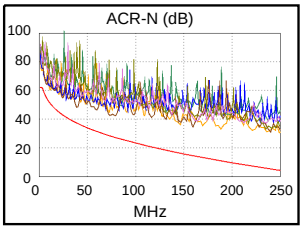


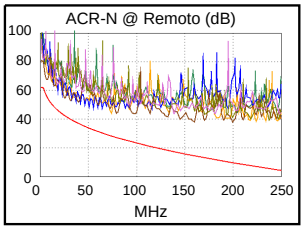


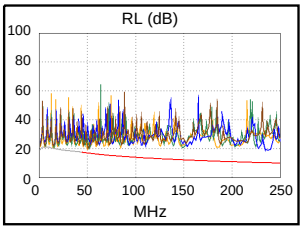


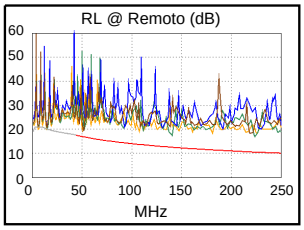












LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-8

Fecha / Hora: 12/30/2017 12:08:29 PM
Paso Libre 1.6 dB (NEXT 36-45)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 45]	43.0
Tiempo de Prop. (ns), Lím. 498	[Par 12]	220
Diferencia Retardo (ns), Lím. 44	[Par 12]	12
Resistencia (ohm.)	[Par 36]	6.6
Pérdida inserción Margen (dB)	[Par 12]	15.5
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	36-45	36-45
NEXT (dB)	1.6	3.4	2.2	3.4
Frec. (MHz)	71.3	229.5	237.5	229.5
Límite (dB)	44.2	35.9	35.7	35.9
Peor Par	36	36	36	36
PS NEXT (dB)	2.3	4.9	2.3	5.2
Frec. (MHz)	239.5	31.5	239.5	246.5
Límite (dB)	33.0	47.5	33.0	32.8

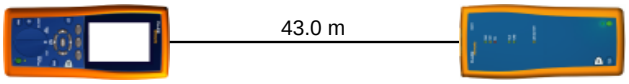
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	45-36	45-36	36-45
ACR-F (dB)	10.3	10.5	12.1	12.9
Frec. (MHz)	98.0	93.3	250.0	250.0
Límite (dB)	24.4	24.8	16.2	16.2
Peor Par	36	36	36	36
PS ACR-F (dB)	11.9	12.8	11.9	12.8
Frec. (MHz)	250.0	1.0	250.0	249.5
Límite (dB)	13.2	61.2	13.2	13.2

N/A	MAIN	SR	MAIN	SR
Peor Par	12-78	12-78	36-45	36-45
ACR-N (dB)	8.1	8.7	18.3	20.4
Frec. (MHz)	19.3	14.4	237.5	246.5
Límite (dB)	45.6	48.7	5.5	4.6
Peor Par	36	12	36	36
PS ACR-N (dB)	8.8	9.1	17.8	20.9
Frec. (MHz)	10.9	14.4	239.5	246.5
Límite (dB)	49.1	46.3	2.7	2.0

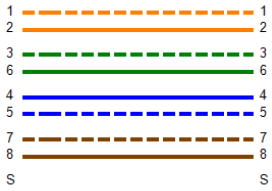
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	12	78
RL (dB)	1.9	2.0	8.4	6.9
Frec. (MHz)	9.9	10.0	192.0	233.0
Límite (dB)	21.0	21.0	11.2	10.3

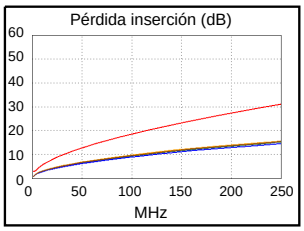
Estándares de Red Compatibles:

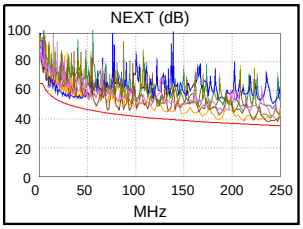
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

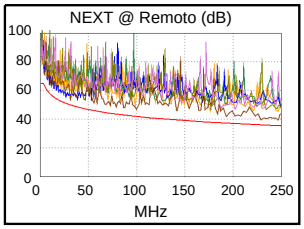


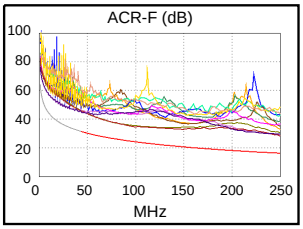
Mapa de Cableado (T568B)
PASA

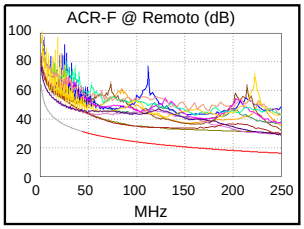


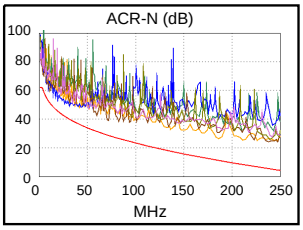


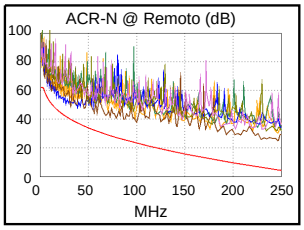


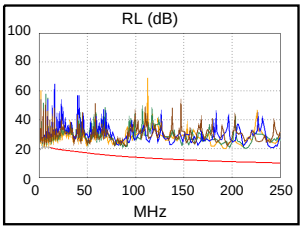


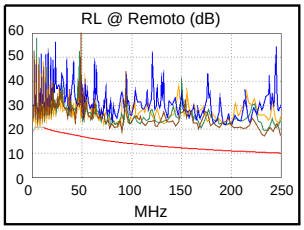












LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-7

Fecha / Hora: 12/30/2017 12:55:45 PM
Paso Libre 0.2 dB (NEXT 36-45)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 45]	67.2
Tiempo de Prop. (ns), Lím. 498	[Par 12]	344
Diferencia Retardo (ns), Lím. 44	[Par 12]	19
Resistencia (ohm.)	[Par 12]	10.6
Pérdida inserción Margen (dB)	[Par 12]	6.9
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	36-45	12-36
NEXT (dB)	0.2*	1.0	1.3	3.1
Frec. (MHz)	38.0	38.0	238.0	185.0
Límite (dB)	48.6	48.6	35.7	37.5
Peor Par	36	36	36	36
PS NEXT (dB)	1.4	3.0	1.5	4.5
Frec. (MHz)	235.0	38.0	248.5	186.5
Límite (dB)	33.2	46.2	32.7	34.8

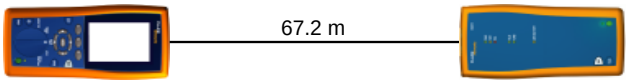
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	45-36	45-36	36-45
ACR-F (dB)	10.3	10.7	10.7	11.6
Frec. (MHz)	204.0	202.5	226.5	226.5
Límite (dB)	18.0	18.1	17.1	17.1
Peor Par	36	36	36	45
PS ACR-F (dB)	11.6	12.1	11.9	12.8
Frec. (MHz)	187.0	188.5	203.5	226.5
Límite (dB)	15.8	15.7	15.0	14.1

N/A	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	12-36	36-45
ACR-N (dB)	2.9	3.2	9.9	13.0
Frec. (MHz)	38.0	18.8	250.0	225.0
Límite (dB)	37.6	45.9	4.2	6.8
Peor Par	36	36	36	36
PS ACR-N (dB)	4.6	4.8	9.0	14.0
Frec. (MHz)	38.0	18.5	248.5	239.5
Límite (dB)	35.1	43.6	1.8	2.7

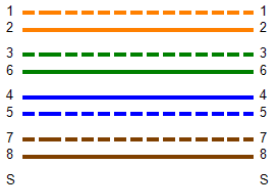
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	45	36
RL (dB)	1.5	1.0*	6.5	6.5
Frec. (MHz)	6.3	6.4	141.0	190.0
Límite (dB)	21.0	21.0	12.5	11.2

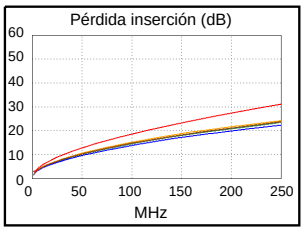
Estándares de Red Compatibles:

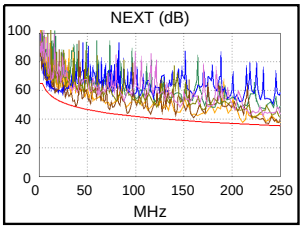
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

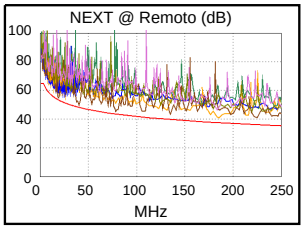


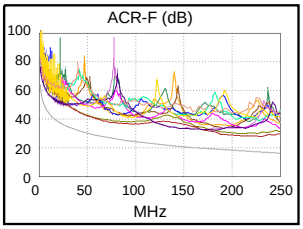
Mapa de Cableado (T568B)
PASA

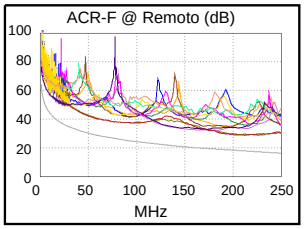


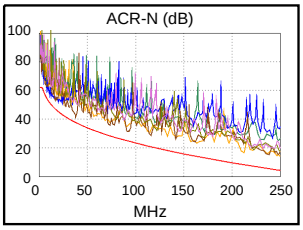


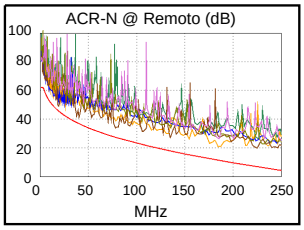


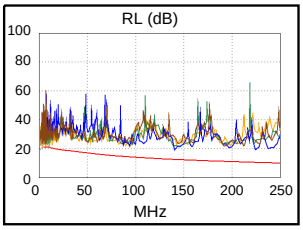


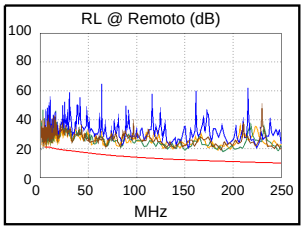












* El margen está dentro de los límites de exactitud del instrumento.

LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-6

Fecha / Hora: 12/30/2017 12:57:35 PM
Paso Libre 1.7 dB (NEXT 12-36)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 45]	69.7
Tiempo de Prop. (ns), Lím. 498	[Par 12]	357
Diferencia Retardo (ns), Lím. 44	[Par 12]	20
Resistencia (ohm.)	[Par 12]	10.9
Pérdida inserción Margen (dB)	[Par 12]	6.0
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	12-36	36-45	12-36	36-45
NEXT (dB)	1.7	2.9	1.7	4.1
Frec. (MHz)	246.5	104.0	246.5	246.0
Límite (dB)	35.4	41.6	35.4	35.5
Peor Par	36	36	36	36
PS NEXT (dB)	1.5	4.3	1.5	5.7
Frec. (MHz)	245.0	16.6	245.0	249.5
Límite (dB)	32.9	52.0	32.9	32.7

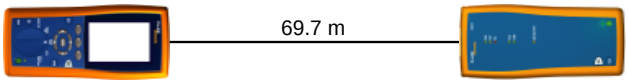
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	36-45	45-36	45-36
ACR-F (dB)	9.6	10.6	9.8	11.6
Frec. (MHz)	187.0	186.5	200.5	222.0
Límite (dB)	18.8	18.8	18.1	17.3
Peor Par	36	36	36	36
PS ACR-F (dB)	10.6	10.5	11.4	11.5
Frec. (MHz)	1.0	1.0	200.5	189.5
Límite (dB)	61.2	61.2	15.1	15.6

N/A	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	12-36	36-45
ACR-N (dB)	4.7	4.9	8.3	12.0
Frec. (MHz)	35.8	16.9	246.5	246.0
Límite (dB)	38.3	47.0	4.6	4.6
Peor Par	36	36	36	36
PS ACR-N (dB)	5.8	5.5	8.2	12.3
Frec. (MHz)	16.9	16.5	246.5	249.5
Límite (dB)	44.6	44.9	2.0	1.7

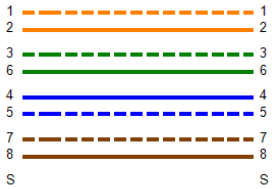
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	45	78
RL (dB)	1.4	1.3	8.3	6.7
Frec. (MHz)	8.9	10.3	204.0	247.0
Límite (dB)	21.0	20.9	10.9	10.1

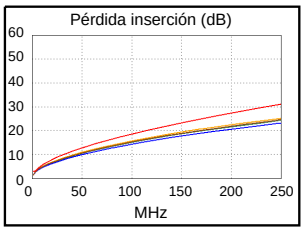
Estándares de Red Compatibles:

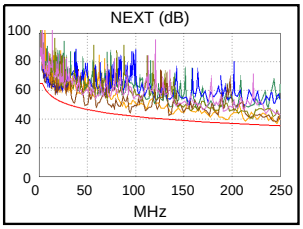
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

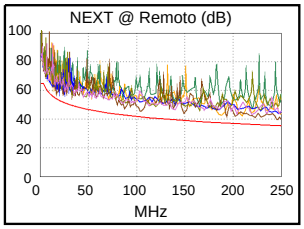


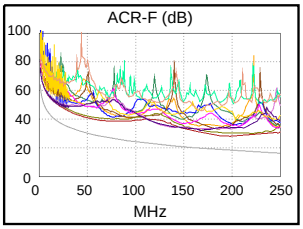
Mapa de Cableado (T568B)
PASA

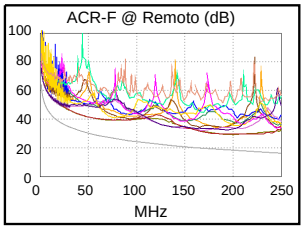


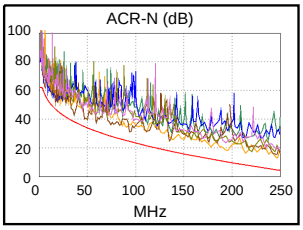


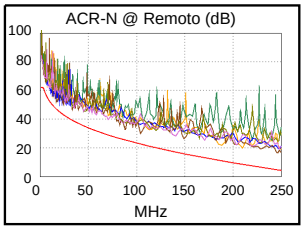


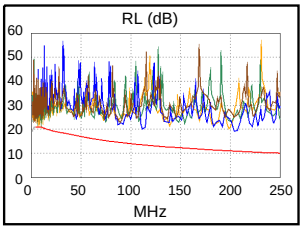


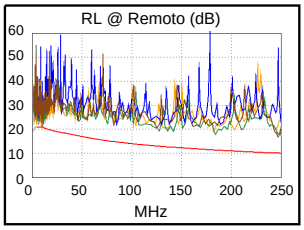












LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-4

Fecha / Hora: 01/02/2018 12:54:21 PM
Paso Libre 1.3 dB (NEXT 36-45)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 45]	72.8
Tiempo de Prop. (ns), Lím. 498	[Par 12]	373
Diferencia Retardo (ns), Lím. 44	[Par 12]	21
Resistencia (ohm.)	[Par 12]	11.3
Pérdida inserción Margen (dB)	[Par 12]	5.0
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	12-36	36-45
NEXT (dB)	1.3	1.5	3.0	4.3
Frec. (MHz)	82.5	39.5	235.5	196.0
Límite (dB)	43.2	48.3	35.8	37.1
Peor Par	36	45	36	36
PS NEXT (dB)	2.2	3.4	2.2	5.7
Frec. (MHz)	235.0	19.5	235.0	224.5
Límite (dB)	33.2	50.8	33.2	33.5

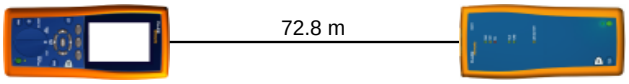
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	36-45	45-36	36-45
ACR-F (dB)	10.8	11.8	11.4	12.6
Frec. (MHz)	168.0	168.0	249.5	249.5
Límite (dB)	19.7	19.7	16.2	16.2
Peor Par	36	36	36	45
PS ACR-F (dB)	10.9	11.0	12.3	13.5
Frec. (MHz)	1.0	1.0	249.5	249.5
Límite (dB)	61.2	61.2	13.2	13.2

N/A	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	12-36	36-45
ACR-N (dB)	4.4	3.0	9.8	11.9
Frec. (MHz)	12.5	19.3	248.0	225.0
Límite (dB)	50.1	45.6	4.4	6.8
Peor Par	36	36	36	36
PS ACR-N (dB)	5.3	4.7	7.8	12.2
Frec. (MHz)	82.5	19.3	235.0	239.5
Límite (dB)	24.0	43.2	3.1	2.7

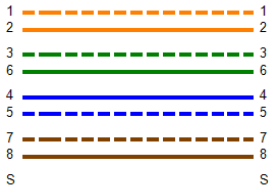
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	36	36
RL (dB)	1.9	1.7	5.8	7.2
Frec. (MHz)	8.5	8.4	135.5	234.5
Límite (dB)	21.0	21.0	12.7	10.3

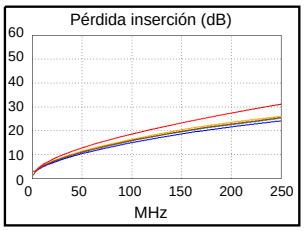
Estándares de Red Compatibles:

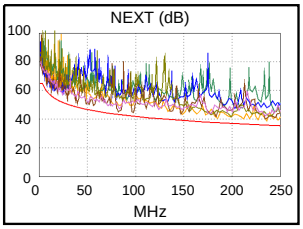
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

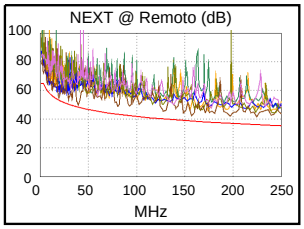


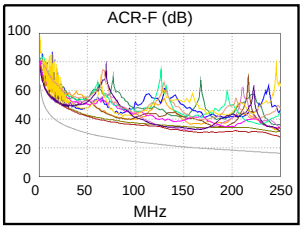
Mapa de Cableado (T568B)
PASA

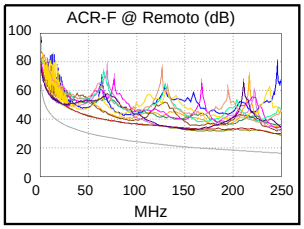


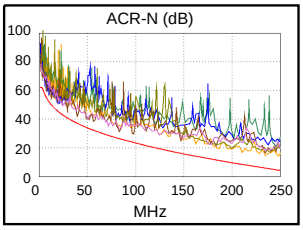


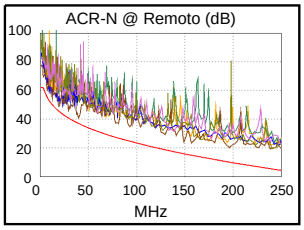


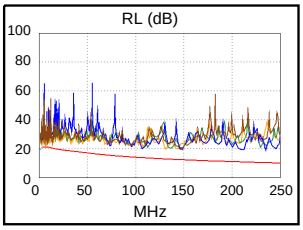


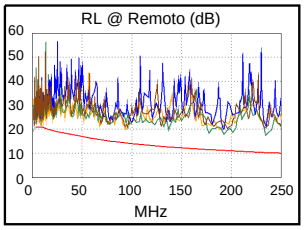












LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: AP-5

Fecha / Hora: 01/02/2018 01:19:06 PM
Paso Libre 1.2 dB (NEXT 36-45)
Limite de Prueba: TIA Cat 6 Perm. Link
Tipo de Cable: Cat 6 U/UTP
NVP: 69.0%

Operador: RAFAEL
Versión de Software: 2.7800
Version de Limites: 1.9500

Sumario de Pruebas: PASA

Modelo: DTX-1800
Principal N/S: 9126090
Remoto N/S: 9126089
Adaptador Principal: DTX-PLA002
Adaptador Remoto: DTX-PLA002

Longitud (m), Lím. 90.0	[Par 45]	65.4
Tiempo de Prop. (ns), Lím. 498	[Par 12]	335
Diferencia Retardo (ns), Lím. 44	[Par 12]	19
Resistencia (ohm.)	[Par 12]	10.4
Pérdida inserción Margen (dB)	[Par 12]	7.5
Frecuencia (MHz)	[Par 12]	250.0
Límite (dB)	[Par 12]	31.1

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	36-45	36-45	36-45
NEXT (dB)	1.2	1.9	1.2	1.9
Frec. (MHz)	250.0	166.0	250.0	166.0
Límite (dB)	35.3	38.3	35.3	38.3
Peor Par	36	36	36	45
PS NEXT (dB)	0.8*	3.8	0.8	4.1
Frec. (MHz)	250.0	144.0	250.0	166.0
Límite (dB)	32.7	36.7	32.7	35.7

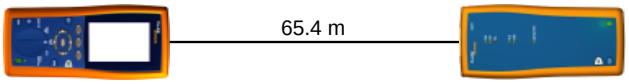
PASA	MAIN	SR	MAIN	SR
Peor Par	45-36	36-45	45-36	36-45
ACR-F (dB)	8.1	9.0	8.1	9.0
Frec. (MHz)	212.0	212.0	213.0	212.0
Límite (dB)	17.7	17.7	17.6	17.7
Peor Par	36	45	36	45
PS ACR-F (dB)	10.3	10.4	10.4	10.4
Frec. (MHz)	187.0	212.0	212.0	213.0
Límite (dB)	15.8	14.7	14.7	14.6

N/A	MAIN	SR	MAIN	SR
Peor Par	12-78	12-78	36-45	36-45
ACR-N (dB)	4.8	5.7	10.3	14.1
Frec. (MHz)	11.0	15.8	250.0	233.0
Límite (dB)	51.4	47.7	4.2	6.0
Peor Par	78	36	36	36
PS ACR-N (dB)	6.3	6.6	9.0	14.9
Frec. (MHz)	11.0	42.0	250.0	233.0
Límite (dB)	49.0	33.8	1.6	3.4

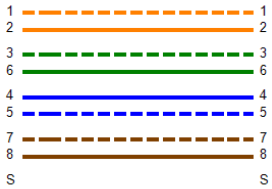
PASA	MAIN	SR	MAIN	SR
Peor Par	12	12	45	12
RL (dB)	1.4	1.7	6.7	4.9
Frec. (MHz)	8.0	6.5	250.0	158.5
Límite (dB)	21.0	21.0	10.0	12.0

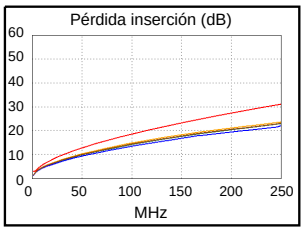
Estándares de Red Compatibles:

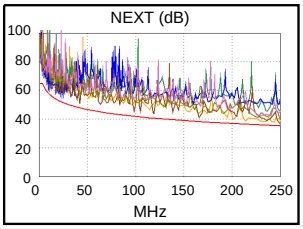
10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

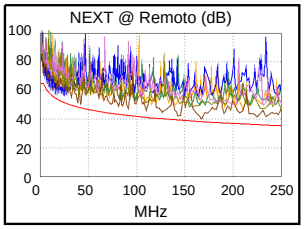


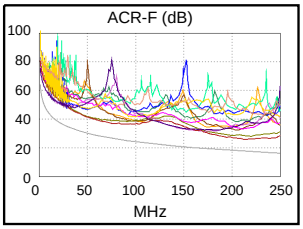
Mapa de Cableado (T568B)
PASA

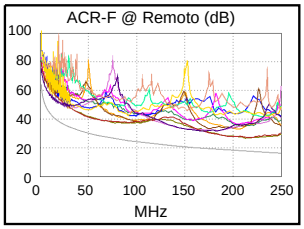


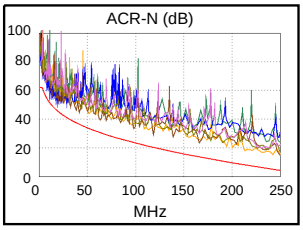


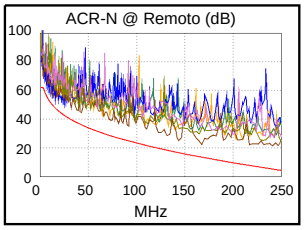


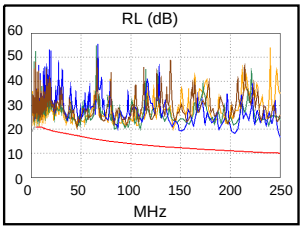


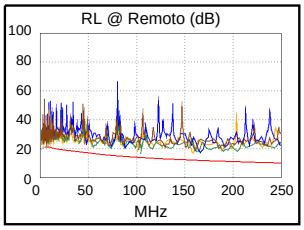












* El margen está dentro de los límites de exactitud del instrumento.

LinkWare™ PC Versión 9.8

Proyecto: CORTIJO-ALAMILLO
cortijo del alamillo.flw

Lugar: SEVILLA

FLUKE networks

8 Plantilla de configuración

```
version 6.5.1.0-4.3.1.0

virtual-controller-country ES

virtual-controller-ip %ip_address_vc%

terminal-access

ntp-server %ip_address_ntp%
clock timezone summer-time

dynamic-radius-proxy

allow-new-aps


routing-profile
route %ip_address_terminadora1% 255.255.255.255 %ip_address_terminadora1%
route %ip_address_terminadora2% 255.255.255.255 %ip_address_terminadora1%


snmp-server community %comunity%


arm
wide-bands 5ghz
80mhz-support
min-tx-power 15
max-tx-power 18
air-time-fairness-mode fair-access
scanning
client-match


syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless


extended-ssid


vpn primary %ip_address_controladora_master%
vpn gre-outside


mgmt-user admin XXXXXXXXXXXX


wlan access-rule default_wired_port_profile
```

```
rule any any match any any any permit

wlan access-rule wired-instant
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit

wlan access-rule LOCAL
rule any any match any any any permit

wlan access-rule ITINERANTE
rule any any match any any any permit

wlan access-rule INVITADOS
rule any any match any any any permit

wlan access-rule tpl-invitados-logon
rule %ip_RADIUS% 255.255.255.255 match tcp 80 80 permit
rule %ip_RADIUS% 255.255.255.255 match tcp 443 443 permit
rule %ip_publica_portal% 255.255.255.255 match tcp 80 80 permit
rule %ip_publica_portal% 255.255.255.255 match tcp 443 443 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit



wlan ssid-profile EMPLEADOS
enable
type employee
essid EMPLEADOS
opmode wpa2-aes
max-authentication-failures 0
vlan 4092
auth-server RADIUS
set-vlan Aruba-User-Role equals ITINERANTE 4092
set-vlan Aruba-User-Role equals LOCAL 20
rf-band all
captive-portal disable
dtim-period 1
broadcast-filter arp
enforce-dhcp
server-load-balancing
radius-accounting
radius-interim-accounting-interval 10
g-min-tx-rate 6
a-min-tx-rate 9
multicast-rate-optimization
dynamic-multicast-optimization
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64

wlan ssid-profile INVITADOS
enable
type guest
essid INVITADOS
```

```
opmode opensystem
max-authentication-failures 0
vlan 4093
auth-server tpl-invitados
set-role-pre-auth tpl-invitados-logon
rf-band all
captive-portal external
mac-authentication
dtim-period 1
broadcast-filter arp
radius-accounting
radius-interim-accounting-interval 10
g-min-tx-rate 6
a-min-tx-rate 9
multicast-rate-optimization
dynamic-multicast-optimization
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64


auth-survivability cache-time-out 24


mgmt-auth-server RADIUS


mgmt-auth-server-local-backup


dpi


wlan auth-server tpl-invitados
ip %ip_RADIUS%
port 1812
acctport 1813
key XXXXXXXXXXXX
rfc3576
cppm-rfc3576-port 3799

wlan auth-server RADIUS
ip %ip_RADIUS%
port 1812
acctport 1813
key XXXXXXXXXXXX
nas-ip %ip_address_vc%
nas-id %hostname%

wlan external-captive-portal
server portalwifi.es
port 443
url "/guest/portal_de_registro.php?_browser=1&apgroup=%hostname%"
auth-text ""
auto-whitelist-disable
https
```

```
blacklist-time 3600
auth-failure-blacklist-time 3600


ids
wireless-containment none


ip dhcp INVITADOS
server-type Centralized,L2
server-vlan 4093
disable-split-tunnel

ip dhcp ITINERANTE
server-type Centralized,L2
server-vlan 4092
disable-split-tunnel


wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x


wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 100
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
auth-server InternalServer
captive-portal disable
no dot1x


enet0-port-profile default_wired_port_profile
enet1-port-profile default_wired_port_profile


uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
```

```
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180


airgroup
disable

airgroupservice airplay
disable
description AirPlay

airgroupservice airprint
disable
description AirPrint
```